## Contents

<table>
<thead>
<tr>
<th>Response</th>
<th>Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Susan Whyble</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Saiph Savage</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>American Hotel &amp; Lodging Association, Chamber Technology Engagement Center, Flex, HR Policy Association, Modern Economy Project, National Council of Chain Restaurants, National Retail Federation, TechNet</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Luke Robles</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>Anonymous1</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Anonymous2</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Dev Purkayastha</td>
<td>12</td>
</tr>
<tr>
<td>8</td>
<td>Birgit Hermann</td>
<td>13</td>
</tr>
<tr>
<td>9</td>
<td>Bonnie Arbuckle</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>Katherine Dander</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>Bill O'Brien</td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td>Jesse Williams</td>
<td>17</td>
</tr>
<tr>
<td>13</td>
<td>John Lowe</td>
<td>18</td>
</tr>
<tr>
<td>14</td>
<td>Diane Matta</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>Michael Madden</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>Elizabeth Watts</td>
<td>21</td>
</tr>
<tr>
<td>17</td>
<td>Bob Lichtenbert</td>
<td>22</td>
</tr>
<tr>
<td>18</td>
<td>Marie Wiggins</td>
<td>23</td>
</tr>
<tr>
<td>19</td>
<td>C D</td>
<td>24</td>
</tr>
<tr>
<td>20</td>
<td>Shauna Gordon-McKeon</td>
<td>27</td>
</tr>
<tr>
<td>21</td>
<td>Richard Smith</td>
<td>29</td>
</tr>
<tr>
<td>22</td>
<td>Susan Blain</td>
<td>30</td>
</tr>
<tr>
<td>23</td>
<td>Kenneth Bryan</td>
<td>31</td>
</tr>
<tr>
<td>24</td>
<td>Pam Letourneau</td>
<td>32</td>
</tr>
<tr>
<td>25</td>
<td>Maryann Becich</td>
<td>33</td>
</tr>
<tr>
<td>26</td>
<td>Joseph Lawson</td>
<td>34</td>
</tr>
<tr>
<td>27</td>
<td>Darrell House</td>
<td>35</td>
</tr>
<tr>
<td>28</td>
<td>Karen Heesch</td>
<td>36</td>
</tr>
<tr>
<td>29</td>
<td>Craig Clark</td>
<td>37</td>
</tr>
<tr>
<td>30</td>
<td>Chas Griffin</td>
<td>38</td>
</tr>
<tr>
<td>31</td>
<td>Don Pew</td>
<td>39</td>
</tr>
<tr>
<td>32</td>
<td>Dan Stanger</td>
<td>40</td>
</tr>
<tr>
<td>33</td>
<td>Jerry Mawhorter</td>
<td>41</td>
</tr>
<tr>
<td>34</td>
<td>CF Massey</td>
<td>42</td>
</tr>
<tr>
<td>35</td>
<td>National Federation of Independent Business (NFIB)</td>
<td>43</td>
</tr>
<tr>
<td>36</td>
<td>John Papandrea</td>
<td>46</td>
</tr>
<tr>
<td>37</td>
<td>Susan Goldstein</td>
<td>47</td>
</tr>
<tr>
<td>38</td>
<td>David Miller</td>
<td>48</td>
</tr>
<tr>
<td>39</td>
<td>Cheryl Militello</td>
<td>49</td>
</tr>
<tr>
<td>Response</td>
<td>Name</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------</td>
<td>------</td>
</tr>
<tr>
<td>40</td>
<td>Allison Fradkin</td>
<td>50</td>
</tr>
<tr>
<td>41</td>
<td>Peter Reimer</td>
<td>51</td>
</tr>
<tr>
<td>42</td>
<td>Elizabeth MacKelvie</td>
<td>52</td>
</tr>
<tr>
<td>43</td>
<td>Peter Jacques</td>
<td>53</td>
</tr>
<tr>
<td>44</td>
<td>Anonymous3</td>
<td>54</td>
</tr>
<tr>
<td>45</td>
<td>John Ahlquist</td>
<td>55</td>
</tr>
<tr>
<td>46</td>
<td>Alex Wawro</td>
<td>58</td>
</tr>
<tr>
<td>47</td>
<td>Kate Bronfenbrenner</td>
<td>59</td>
</tr>
<tr>
<td>48</td>
<td>Merve Hickok</td>
<td>62</td>
</tr>
<tr>
<td>49</td>
<td>ActivTrak</td>
<td>78</td>
</tr>
<tr>
<td>50</td>
<td>Theodore Wiggin</td>
<td>89</td>
</tr>
<tr>
<td>51</td>
<td>Anonymous4</td>
<td>143</td>
</tr>
<tr>
<td>52</td>
<td>Saiph Savage</td>
<td>145</td>
</tr>
<tr>
<td>53</td>
<td>Catherine Clifton</td>
<td>148</td>
</tr>
<tr>
<td>54</td>
<td>Jerome Maynard</td>
<td>149</td>
</tr>
<tr>
<td>55</td>
<td>Hugh Keleher</td>
<td>150</td>
</tr>
<tr>
<td>56</td>
<td>Thalia Lubin</td>
<td>151</td>
</tr>
<tr>
<td>57</td>
<td>Patricia Baecker</td>
<td>152</td>
</tr>
<tr>
<td>58</td>
<td>UNITE HERE</td>
<td>153</td>
</tr>
<tr>
<td>59</td>
<td>Ted Silen</td>
<td>158</td>
</tr>
<tr>
<td>60</td>
<td>James Dawson</td>
<td>159</td>
</tr>
<tr>
<td>61</td>
<td>Donna Selquist</td>
<td>160</td>
</tr>
<tr>
<td>62</td>
<td>Alex Stavis</td>
<td>161</td>
</tr>
<tr>
<td>63</td>
<td>Rita Meuer</td>
<td>162</td>
</tr>
<tr>
<td>64</td>
<td>Matt Brzezinski</td>
<td>163</td>
</tr>
<tr>
<td>65</td>
<td>Mark Williams</td>
<td>164</td>
</tr>
<tr>
<td>66</td>
<td>Gloria McClintock</td>
<td>165</td>
</tr>
<tr>
<td>67</td>
<td>Javier Del Valle</td>
<td>166</td>
</tr>
<tr>
<td>68</td>
<td>Russell Novkov</td>
<td>167</td>
</tr>
<tr>
<td>69</td>
<td>Leona McCann</td>
<td>168</td>
</tr>
<tr>
<td>70</td>
<td>Robert Fingerman</td>
<td>169</td>
</tr>
<tr>
<td>71</td>
<td>Athena Addams</td>
<td>170</td>
</tr>
<tr>
<td>72</td>
<td>Diane Kraft</td>
<td>171</td>
</tr>
<tr>
<td>73</td>
<td>Mark Hayduke Grenard</td>
<td>172</td>
</tr>
<tr>
<td>74</td>
<td>Doris Ashbrook</td>
<td>173</td>
</tr>
<tr>
<td>75</td>
<td>James Deshotels</td>
<td>174</td>
</tr>
<tr>
<td>76</td>
<td>Lascinda Goetschius</td>
<td>175</td>
</tr>
<tr>
<td>77</td>
<td>I Engle</td>
<td>176</td>
</tr>
<tr>
<td>78</td>
<td>Kevin Walsh</td>
<td>177</td>
</tr>
<tr>
<td>79</td>
<td>Mary Casey</td>
<td>178</td>
</tr>
<tr>
<td>80</td>
<td>Stephen Anderson</td>
<td>179</td>
</tr>
<tr>
<td>81</td>
<td>S Robertson</td>
<td>180</td>
</tr>
<tr>
<td>82</td>
<td>Frank Belcastro</td>
<td>181</td>
</tr>
<tr>
<td>83</td>
<td>Aleks Kosowicz</td>
<td>182</td>
</tr>
<tr>
<td>84</td>
<td>Armando Garcia</td>
<td>183</td>
</tr>
<tr>
<td>Response</td>
<td>Name</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>85</td>
<td>Tsee Lee</td>
<td>184</td>
</tr>
<tr>
<td>86</td>
<td>Joyce Frohn</td>
<td>185</td>
</tr>
<tr>
<td>87</td>
<td>Bill O'Brien</td>
<td>186</td>
</tr>
<tr>
<td>88</td>
<td>Alice Polesky</td>
<td>187</td>
</tr>
<tr>
<td>89</td>
<td>Gary Charles</td>
<td>188</td>
</tr>
<tr>
<td>90</td>
<td>Jean Bails</td>
<td>189</td>
</tr>
<tr>
<td>91</td>
<td>Pat Magrath</td>
<td>190</td>
</tr>
<tr>
<td>92</td>
<td>Virgene Link-New</td>
<td>191</td>
</tr>
<tr>
<td>93</td>
<td>SHRM</td>
<td>192</td>
</tr>
<tr>
<td>94</td>
<td>Elyette Weinstein</td>
<td>195</td>
</tr>
<tr>
<td>95</td>
<td>Mary Sullivan</td>
<td>196</td>
</tr>
<tr>
<td>96</td>
<td>Lynette Bech</td>
<td>197</td>
</tr>
<tr>
<td>97</td>
<td>Christopher Vota</td>
<td>198</td>
</tr>
<tr>
<td>98</td>
<td>Evelyn Fraser</td>
<td>199</td>
</tr>
<tr>
<td>99</td>
<td>United Steelworkers (USW)</td>
<td>200</td>
</tr>
<tr>
<td>100</td>
<td>Judith Ackerman</td>
<td>204</td>
</tr>
<tr>
<td>101</td>
<td>Jim Piascik</td>
<td>205</td>
</tr>
<tr>
<td>102</td>
<td>Eric Huntley</td>
<td>206</td>
</tr>
<tr>
<td>103</td>
<td>Elizabeth Seltzer</td>
<td>207</td>
</tr>
<tr>
<td>104</td>
<td>Robert Thomasson</td>
<td>208</td>
</tr>
<tr>
<td>105</td>
<td>Kirk Bails</td>
<td>209</td>
</tr>
<tr>
<td>106</td>
<td>Sherrill Futreell</td>
<td>210</td>
</tr>
<tr>
<td>107</td>
<td>Freya Harris</td>
<td>211</td>
</tr>
<tr>
<td>108</td>
<td>Deborah Wolf</td>
<td>212</td>
</tr>
<tr>
<td>109</td>
<td>B Chan</td>
<td>213</td>
</tr>
<tr>
<td>110</td>
<td>Sharon Paltin</td>
<td>214</td>
</tr>
<tr>
<td>111</td>
<td>Jarrod Simmons</td>
<td>215</td>
</tr>
<tr>
<td>112</td>
<td>Utkarsh Nath</td>
<td>216</td>
</tr>
<tr>
<td>113</td>
<td>Rebecca Berlant</td>
<td>217</td>
</tr>
<tr>
<td>114</td>
<td>Dan DiLeva</td>
<td>218</td>
</tr>
<tr>
<td>115</td>
<td>Asphodel Denning</td>
<td>219</td>
</tr>
<tr>
<td>116</td>
<td>Annetta Winkle</td>
<td>220</td>
</tr>
<tr>
<td>117</td>
<td>Karl Moore</td>
<td>221</td>
</tr>
<tr>
<td>118</td>
<td>John Dervin</td>
<td>222</td>
</tr>
<tr>
<td>119</td>
<td>Alisa Hermann-Wu</td>
<td>223</td>
</tr>
<tr>
<td>120</td>
<td>Kate Hermann-Wu</td>
<td>224</td>
</tr>
<tr>
<td>121</td>
<td>Emily Willoughby</td>
<td>225</td>
</tr>
<tr>
<td>122</td>
<td>Tammy Lettieri</td>
<td>226</td>
</tr>
<tr>
<td>123</td>
<td>Howard Lepzelter</td>
<td>227</td>
</tr>
<tr>
<td>124</td>
<td>Rick Wojdowski</td>
<td>228</td>
</tr>
<tr>
<td>125</td>
<td>Dean Sigler</td>
<td>229</td>
</tr>
<tr>
<td>126</td>
<td>Dean Rumiantseva</td>
<td>230</td>
</tr>
<tr>
<td>127</td>
<td>Susan McCorry</td>
<td>231</td>
</tr>
<tr>
<td>128</td>
<td>Maria Moreno</td>
<td>232</td>
</tr>
<tr>
<td>129</td>
<td>Charles Wright</td>
<td>233</td>
</tr>
<tr>
<td>Response</td>
<td>Name</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>130</td>
<td>Ron Strochlic</td>
<td>234</td>
</tr>
<tr>
<td>131</td>
<td>Lily Mejia</td>
<td>235</td>
</tr>
<tr>
<td>132</td>
<td>Anna Louise Fontaine</td>
<td>236</td>
</tr>
<tr>
<td>133</td>
<td>Mark Hayduke Grenard</td>
<td>237</td>
</tr>
<tr>
<td>134</td>
<td>Brent Rocks</td>
<td>238</td>
</tr>
<tr>
<td>135</td>
<td>David Lavender</td>
<td>239</td>
</tr>
<tr>
<td>136</td>
<td>Brett O'Sullivan</td>
<td>240</td>
</tr>
<tr>
<td>137</td>
<td>John Oda</td>
<td>241</td>
</tr>
<tr>
<td>138</td>
<td>Jenn Crum</td>
<td>242</td>
</tr>
<tr>
<td>139</td>
<td>Linda Heath</td>
<td>243</td>
</tr>
<tr>
<td>140</td>
<td>Sharon Goel</td>
<td>244</td>
</tr>
<tr>
<td>141</td>
<td>John Sonin</td>
<td>245</td>
</tr>
<tr>
<td>142</td>
<td>Antonino Erba</td>
<td>246</td>
</tr>
<tr>
<td>143</td>
<td>David Amrod</td>
<td>247</td>
</tr>
<tr>
<td>144</td>
<td>Diane Olson Schmidt</td>
<td>248</td>
</tr>
<tr>
<td>145</td>
<td>AvaSure LLC</td>
<td>249</td>
</tr>
<tr>
<td>146</td>
<td>Alexandre Papajak</td>
<td>252</td>
</tr>
<tr>
<td>147</td>
<td>Heather Touhey</td>
<td>296</td>
</tr>
<tr>
<td>148</td>
<td>National Treasury Employees Union (NTEU)</td>
<td>302</td>
</tr>
<tr>
<td>149</td>
<td>the Computer &amp; Communications Industry Association (CCIA)</td>
<td>310</td>
</tr>
<tr>
<td>150</td>
<td>Bipartisan Policy Center</td>
<td>318</td>
</tr>
<tr>
<td>151</td>
<td>Center for AI and Digital Policy</td>
<td>327</td>
</tr>
<tr>
<td>152</td>
<td>Owner-Operator Independent Drivers Association</td>
<td>337</td>
</tr>
<tr>
<td>153</td>
<td>ACM US Technology Policy Committee</td>
<td>341</td>
</tr>
<tr>
<td>154</td>
<td>The Retail, Wholesale and Department Store Union, RWDSU</td>
<td>352</td>
</tr>
<tr>
<td>155</td>
<td>Economic Policy Institute</td>
<td>356</td>
</tr>
<tr>
<td>156</td>
<td>Pegah Moradi</td>
<td>392</td>
</tr>
<tr>
<td>157</td>
<td>Electronic Privacy Information Center (EPIC)</td>
<td>424</td>
</tr>
<tr>
<td>158</td>
<td>International Federation of Professional and Technical Engineers</td>
<td>429</td>
</tr>
<tr>
<td>159</td>
<td>Elizabeth H</td>
<td>437</td>
</tr>
<tr>
<td>160</td>
<td>Eric Robinson</td>
<td>450</td>
</tr>
<tr>
<td>161</td>
<td>Karen Boehler</td>
<td>451</td>
</tr>
<tr>
<td>162</td>
<td>Anonymous5</td>
<td>452</td>
</tr>
<tr>
<td>163</td>
<td>Retail, Wholesale and Department Store Union (RWDSU/UFCW)</td>
<td>453</td>
</tr>
<tr>
<td>164</td>
<td>Data &amp; Society Research Institute</td>
<td>455</td>
</tr>
<tr>
<td>165</td>
<td>HR Policy Association</td>
<td>474</td>
</tr>
<tr>
<td>166</td>
<td>The Arc of Frederick County</td>
<td>483</td>
</tr>
<tr>
<td>167</td>
<td>AFL-CIO Technology Institute</td>
<td>485</td>
</tr>
<tr>
<td>168</td>
<td>Yesenia Barrera</td>
<td>528</td>
</tr>
<tr>
<td>169</td>
<td>Center for Democracy &amp; Technology, et al.</td>
<td>530</td>
</tr>
<tr>
<td>170</td>
<td>Flex</td>
<td>555</td>
</tr>
<tr>
<td>171</td>
<td>American Foundation for the Blind</td>
<td>570</td>
</tr>
<tr>
<td>172</td>
<td>National Employment Law Project</td>
<td>581</td>
</tr>
<tr>
<td>173</td>
<td>TechNet</td>
<td>598</td>
</tr>
<tr>
<td>174</td>
<td>Khali Jama</td>
<td>605</td>
</tr>
<tr>
<td>Response</td>
<td>Name</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>175</td>
<td>Drema Montgomery</td>
<td>608</td>
</tr>
<tr>
<td>176</td>
<td>Partnership on AI</td>
<td>609</td>
</tr>
<tr>
<td>177</td>
<td>The Center for Law and Social Policy</td>
<td>715</td>
</tr>
<tr>
<td>178</td>
<td>National Partnership for Women &amp; Families</td>
<td>732</td>
</tr>
<tr>
<td>179</td>
<td>UC Berkeley Labor Center</td>
<td>745</td>
</tr>
<tr>
<td>180</td>
<td>Lilly Irani</td>
<td>864</td>
</tr>
<tr>
<td>181</td>
<td>Turkopticon</td>
<td>892</td>
</tr>
<tr>
<td>182</td>
<td>Jennifer Crane</td>
<td>902</td>
</tr>
<tr>
<td>183</td>
<td>National Domestic Workers Alliance</td>
<td>904</td>
</tr>
<tr>
<td>184</td>
<td>Communications Workers of America</td>
<td>913</td>
</tr>
<tr>
<td>185</td>
<td>Action Center on Race and the Economy</td>
<td>927</td>
</tr>
<tr>
<td>186</td>
<td>Ashley Gjovik</td>
<td>943</td>
</tr>
<tr>
<td>187</td>
<td>Public Citizen</td>
<td>991</td>
</tr>
<tr>
<td>188</td>
<td>Jobs With Justice</td>
<td>1000</td>
</tr>
<tr>
<td>189</td>
<td>Service Employees International Union</td>
<td>1004</td>
</tr>
<tr>
<td>190</td>
<td>Towards Justice</td>
<td>1011</td>
</tr>
<tr>
<td>191</td>
<td>National Nurses United</td>
<td>1023</td>
</tr>
<tr>
<td>192</td>
<td>Athena Coalition</td>
<td>1107</td>
</tr>
<tr>
<td>193</td>
<td>National Women's Law Center</td>
<td>1140</td>
</tr>
<tr>
<td>194</td>
<td>United Food and Commercial Workers International Union</td>
<td>1154</td>
</tr>
<tr>
<td>195</td>
<td>Mohamed Farah Hassan</td>
<td>1160</td>
</tr>
<tr>
<td>196</td>
<td>The U.S. Chamber of Commerce's Technology Engagement Center</td>
<td>1162</td>
</tr>
<tr>
<td>197</td>
<td>Knowing Machines Research Group</td>
<td>1248</td>
</tr>
<tr>
<td>198</td>
<td>TechEquity Collaborative</td>
<td>1259</td>
</tr>
<tr>
<td>199</td>
<td>PowerSwitch Action, Chicago Gig Alliance/The People's Lobby,</td>
<td>1275</td>
</tr>
<tr>
<td></td>
<td>Colorado Independent Drivers United-CWA, Gig Workers Rising</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>Prime</td>
<td>1298</td>
</tr>
<tr>
<td>201</td>
<td>Vikram Bhargava</td>
<td>1299</td>
</tr>
<tr>
<td>202</td>
<td>McFadden</td>
<td>1330</td>
</tr>
<tr>
<td>203</td>
<td>Adam</td>
<td>1331</td>
</tr>
<tr>
<td>204</td>
<td>Sean Castillo</td>
<td>1332</td>
</tr>
<tr>
<td>205</td>
<td>Christina Raley</td>
<td>1333</td>
</tr>
<tr>
<td>206</td>
<td>Matt Muscarnera</td>
<td>1334</td>
</tr>
<tr>
<td>207</td>
<td>Joe Fowler</td>
<td>1335</td>
</tr>
<tr>
<td>208</td>
<td>Nicholas Lawson</td>
<td>1336</td>
</tr>
<tr>
<td>209</td>
<td>Melodi Dincer, Kate Crawford, Jason Schultz</td>
<td>1387</td>
</tr>
<tr>
<td>210</td>
<td>Human Computer Interaction Institute, Carnegie Mellon University</td>
<td>1397</td>
</tr>
<tr>
<td>211</td>
<td>Coworker.org</td>
<td>1401</td>
</tr>
<tr>
<td>212</td>
<td>EU-based ecosystem</td>
<td>1410</td>
</tr>
<tr>
<td>213</td>
<td>1E/Wakefield Research</td>
<td>1433</td>
</tr>
</tbody>
</table>
General Comment

I work in an AT&T call center and recognize that I am monitored from the moment I walk into the building to the minute I walk out. I am concerned that instead of enhancing my work experience, AI will be used to replace my position once developers reach the point that AI ineffectively do my job. From a business and profits perspective, AI, once fully developed, will be a cheap and inhuman replacement for the customer service I deliver. I believe that regulations that curtail businesses ability to replace human workers is a necessary move on our government's part to protect the income security of human workers.
PUBLIC SUBMISSION

**Docket:** OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

**Comment On:** OSTP TECH 2023 0004 0001
Request for Information; Automated Worker Surveillance and Management

**Document:** OSTP TECH 2023 0004 DRAFT 0002
Comment on FR Doc # 2023-09353

---

**Submitter Information**

**Name:** Saiph Savage

**Address:**

**Email:** [Redacted]

---

**General Comment**

I think it's crucial to address the protection of workers' rights in the context of sousveillance. Sousveillance refers to workers who actively monitor and document the actions of their bosses or employers, often with the aim of exposing workplace injustices. However, it's important to acknowledge the potential risks that workers, who practice sousveillance, face. Companies or employers could potentially take legal action against workers collecting data about them or enforce non-disclosure agreements that restrict workers' ability to document abuses.

To safeguard workers engaging in sousveillance, we need to establish mechanisms that prevent job loss or retaliation from the company. It's also important to consider how the government can ensure the anonymity of sousveillance tools, ensuring that workers aren't put in danger when utilizing such technologies.

For further context, I am Dr. Saiph Savage, an Assistant Professor at Northeastern University specializing in research on sousveillance systems for gig workers. By addressing these concerns, we could create a more supportive environment that protects and empowers workers involved in sousveillance, fostering greater workplace transparency and accountability.
On behalf of the National Retail Federation, Flex, the American Hotel & Lodging Association, Chamber Technology Engagement Center, HR Policy Association, Modern Economy Project, National Council of Chain Restaurants, and TechNet, please find the attached letter respectfully requesting a 60 day extension to the comment period.
May 24, 2023

Mr. Alan Mislove
Assistant Director for Data and Democracy
Office of Science and Technology Policy
Washington, DC  20500

Re: Request for Comment Period Extension; Request for Information; “Automated Worker Surveillance and Management” (88 FR 27,932)

The undersigned organizations respectfully request a 60-day extension to the comment period on the Office of Science and Technology Policy’s (OSTP) notice of request for information (RFI) on Automated Worker Surveillance and Management, which was published in the Federal Register on May 3, 2023.

The RFI seeks input from the public on the prevalence, uses and purposes, and deployment of automated worker surveillance and management systems. OSTP poses a number of questions to solicit information pertaining to 1) worker experiences with automated worker surveillance and management systems; 2) employer and business experiences implementing or using automated worker surveillance and management systems; 3) technology developer and vendor experiences developing and distributing automated worker surveillance and management systems; 4) data and research relevant to automated worker surveillance and management systems across industries, occupations, and regions; and 5) policies, practices, or standards that the federal government should consider related to automated worker surveillance and management systems.

The existing 43-day comment period poses challenges for parties who wish to submit comments to the RFI. As OSTP notes, these technologies and systems have developed over recent years and across a variety of contexts. Additionally, the complexity of the technology central to OSTP’s focus, combined with the RFI’s comprehensive set of questions, warrants deliberate consideration from all affected stakeholders. An extension to the comment period would afford all parties the opportunity to conduct this inquiry and collect the information needed to develop substantive comments in response to the RFI.

Therefore, the undersigned organizations strongly urge OSTP to provide an additional 60-day extension to the comment period. Doing so will ensure all stakeholders have the opportunity to submit thoughtful and comprehensive comments.

Respectfully submitted,

American Hotel & Lodging Association
Chamber Technology Engagement Center
Flex
HR Policy Association
Modern Economy Project
National Council of Chain Restaurants
National Retail Federation
TechNet
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0004
Comment on FR Doc # 2023-09353

Submitter Information

Name: Luke Robles
Address:
Email: [redacted]

General Comment

See attached PDF file

Attachments

Comments
a. The type of work you do (e.g., describe the relevant job, employer, and industry);

My job title is Content Moderation for a large social media company. I work for them through a different company, a call center who hires moderators for the client.

b. Whether you are a member of a labor union;

I am not a part of a union and would like for my workplace to unionize.

c. The type of automated surveillance or management you have experienced, including the location of the monitoring technology (such as an app you had to use or download; a device you had to use, carry, or wear; or a camera that monitors you);

I was sent a company computer with a webcam and required to have it on at all times (except for breaks). The computer requires me to login to my user profile through a VPN, I then have to input a number passcode from an authentication app from my phone, and once I have logged in, I am required to scan my facial biometrics. Once the lengthy verification login process is done, I am on camera all day. The webcam monitoring software uses an AI to track what is caught on camera, looking for violations. Certain violations are known to us, such as pointing phone at screen or leaving the desk, but no further information is told to us about all violations the AI is looking for and what else is the AI tracking.

d. Whether the automated surveillance or management was used during a labor organizing drive;

No.

e. Whether and when your employer informed you about their use of automated worker surveillance and management systems;

Yes, a short notice was given as a requirement to remain WFH.

f. Whether you (or, if relevant, your representative, like a labor union) have any input or control over how, where, and over what automated surveillance occurs;

No, I have no input.

g. Whether you know how the data generated by surveillance is used for management or other purposes (including purposes related to employment or labor market competition);

No, I don’t know what happens to my facial biometrics that the AI scans for.
h. Whether you (or, if relevant, your representative, like a labor union) have any visibility into the data collected on you or how it is used, including whether data on you collected by surveillance can be shared with other companies, trade groups, or third parties;

No, I don’t know what data is used or what it is used for or if it is being shared with third parties.

i. How the use of automated surveillance and management systems has changed how you do your job or how your employer treated you at your job;

The job is already very mentally taxing and being on camera all day has me incredibly fatigued.

j. Whether your employer has used information from an automated surveillance and management system in support of any discipline against you—and if so, what the action was, how and when you were informed, and what information was provided to you or your representative (such as a labor union);

Not yet.

k. How automated surveillance and management has affected you—whether positively or negatively—including any economic, safety, physical, mental, and emotional impacts;

Badly, my job in content moderation means I see some really terrible videos and being on camera makes me feel even worse. I feel as if my employer doesn’t trust me and is affecting my work output.

l. How automated surveillance and management systems have affected your workplace rights, including rights around collective action, labor organizing, collective bargaining, pay, reasonable accommodations, health and safety, discrimination, and harassment—or your expectation of retaliation when exercising these rights;

I can’t communicate with my coworkers that continue to work on-site, unable to organize and left out of being told news, such as on-site employees being granted a ~$1 raise.

m. How these systems have impacted your non-working hours, personal time, or the privacy of other members of your household;

I have had to disconnect the camera from work computer as I feared the system spying on me in my personal time.

n. If you are disabled or have a health condition, how automated surveillance and management systems have impacted or may impact your use of reasonable accommodations; such as assistive technology or accessibility features of software or breaks, or affected your ability to keep information about your condition private from your employer, supervisor, or coworkers;
o. If you are disabled or have a health condition, how automated surveillance and management systems have affected performance reviews or other management activities, or concerns about how these systems may affect performance reviews or how your management treats you; and

p. Whether you work for an employer that receives Federal funds (for instance, as a Federal contractor).

(b) (6) My company required all employees to return to office. I feel like my performance is under extra scrutiny, especially tracking our (WFH employees) screens all day. I used to be able to take small breaks to stretch (b) (6) and gather myself after a bad video but now I am strictly unable to leave my seat and am forced to remain in frame.
It would be worth investigating the usage of Performance Improvement Plans within tech companies to find justification for employees who have spoken out against the company (either publicly, internally or privately) to be terminated. These plans are usually put into place after monitoring software picks up key words in people's messages - even when apparently private - and can even go as far as checking spoken transcripts of meetings for the same. This is where a lot of these PIPs begin their life and effectively establish a stifling of various forms of criticism of the corporation.
In reference to assets like Bard, the AI engine has the ability to automate a CIA document for sex offense and Judicial proof of sentinel photogrammetry for basic Constitutional protection. Please have AI setup worksets for compliance and employee proof of location for Judicially approved management, including jobsite related location.
General Comment

I'm an experienced software engineer who has worked in many environments - large tech firms such as Google, smaller firms, as a startup cofounder, and as a freelance worker. In all of my experiences, worker autonomy and a culture of open accountability is what led to higher engineering standards and economic growth. The practice of software engineering management has struggled through iterations of OKR based goal-setting [1] to focus on actual business goals (Outcomes), as opposed to specific metrics. Automated surveillance can only capture the latter.

While working as an independent contractor with a financial platform, software engineers were given broad autonomy, and as a freelance worker specifically, care was taken that my work was defined as objective based, rather than with fine grained control. However, the workspace was co-housed with call center workers who were central to the business of the company, but under an different set of hostile surveillance and regulations (The call center workers were also a more racially and culturally diverse body of workers.) The result was corrosive: as call center workers were cut off and dis-incentivized from the company as a whole, the feedback cycle of software development [2]. The engineering body, despite its separate culture, could not retain talent and could not attain the dynamism of its peer companies.

For industries to move towards mass autonomous surveillance would be a waste of economic potential and opportunity

Public Submission

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0008
Comment on FR Doc # 2023-09353

Submitter Information

Name: Birgit Hermann
Address: [Redacted]

General Comment

Please don’t do this!
Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0010
Comment on FR Doc # 2023-09353

Submitter Information

Name: Katherine Dander
Address: United States,

General Comment

Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
Workers do not need to be monitored on camera on the job!
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0012
Comment on FR Doc # 2023-09353

Submitter Information

Name: Jesse Williams
Address: United States,

General Comment

No surveillance!
General Comment

Automated Worker Surveillance and Management poses an unacceptable risk to individuals. Even though employers hope to use it to "manage supply chains, improve health and safety, or make other informed business decisions," the potential for abuse is ripe. An employee should be judged by the quality of their work, not by number keystrokes, eye movements (many of which are unconscious), how quickly they move around facilities. The next step on this slippery slope is brainwave data captured from headgear and earphones (it sounds sci-fi, but there are already items on the market that do this).

Workers consistently have the short end of the stick in the USA, where we have decided that it is more important to ensure the longevity of already-established businesses and industries in lieu of a strong social safety net (PPP loans, for example) allowing employers to forego trust and actual management of employees by using invasive technology would make the tenuous situations workers already have even worse.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0015
Comment on FR Doc # 2023-09353

Submitter Information

Name: Diane Matta
Address: United States,

General Comment

No one wants to be tracked 24/7. Leave people in peace.
The AI restaurant layout manager disregards the human element…we need a balance that respects our health and safety.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0017
Comment on FR Doc # 2023-09353

Submitter Information

Name: Elizabeth Watts
Address: United States,

General Comment

Invasion of privacy!
General Comment

Please stop your computer evaluations.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECHII-2023-0004-DRAFT-0019
Comment on FR Doc # 2023-09353

Submitter Information

Name: Marie Wiggins
Address: United States,

General Comment

The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety.
I spent 7 years working in a call center at a financial institution doing customer support, sales, and retirement planning. Regardless of the role, a huge amount of data was collected about my activities throughout the day. A couple examples:

Schedule adherence: our schedules were meted out at the beginning of the day, and if someone signed in or out a few minutes late, this was noted and sent to their manager. Being out of adherence was grounds for discipline, and people went to great lengths to stay on schedule. If you got a call from your kid’s school or your bank, you couldn’t simply sign out and take the call. I and almost everyone I knew there frequently held our bladders for an uncomfortably long time because we didn’t have a break scheduled. I would not be able to do that job today.

If a customer kept us on the phone 20 minutes into our lunch break, we would still sign back in at the scheduled time and not take our full government-mandated break. Due to the strictness of the adherence policy, and its incompatibility with a number of health conditions, pregnant people, single parents with young kids, and disabled people did not last long in these job roles.

Screen-captured calls: all workers knew that some percentage of our calls would be screen-captured too, and that this could happen at any time, without our knowing. Because our employers could capture data from our monitors at any time, we were not safe to conduct private conversations over email or instant messenger (both of which were also logged and monitored). If you were waiting on hold with another department for 15 minutes, you couldn’t do anything non-work-related on your computer to pass the time such as reading the news or sending personal email. Before smartphones, this meant no communicating with our family members except on our breaks, which as stated earlier, were limited. One time I made the mistake of responding to an instant message from a colleague while waiting for a customer to come back with some information I’d requested. The call was screen-captured and my manager screenshot my instant message and sent it to me in an email with a “??? please see me” in the subject line. It wasn’t an
inappropriate comment, but I was disciplined for it anyway.

There are a number of other metrics that, like the above, exist in the name of “quality customer service” but are dehumanizing and inhumane. These metrics were fed into a spreadsheet and the whole team and department stack-ranked and compared to one another. Everyone could see if you were at the bottom of the pack, even if the reason you were there was something out of your control, such as needing to go to the bathroom when you didn’t have a scheduled break, or a customer verbally abusing you for longer than the 5 minute average handle time.

Working in certain roles in the financial industry opens you up to other privacy violations beyond metrics. When I started my job, I had to give my fingerprints to FINRA against my will. I was also forced to list out my last ten years’ of home addresses, jobs, and criminal record. It also associates you with any past names you may have had, a huge safety risk for victims of domestic abuse and LGBTQ+. All of this information is made available to the public if you are a registered representative. That means any member of the public can go on FINRA’s brokercheck site, look up the name of the customer service rep they talked to (we always had to give a full first and last name), and find out a good deal of identifying information. It also gives the public access to the representative’s first-hand explanation of their criminal record.

I also spent 8 years in Trust and Safety, most of which time involved content moderation. We had to use our personal computers for the first couple years, and were tracked by our keyboard touches. Employer could see, for example, that we exceeded the goal of 100 actions per hour, but if we met the goal within the first half hour and then stopped, we were disciplined for “not working” the full hour, despite exceeding the stated goals. My good friend used to work for a large moderation company that required such a high number of touches per hour that my friend was working off the clock and skipping their breaks. They have ME/CFS so the lack of rest ended up triggering a relapse, and they had to stop working. Many people in my content moderation job also worked off the clock and through their breaks.

see attached for final thoughts

---

Attachments

Screenshot from 2023-06-12 21-24-02
was working off the clock and skipping their breaks. They have ME/CFS so the lack of rest ended up triggering a relapse, and they had to stop working. Many people in my content moderation job also worked off the clock and through their breaks.

My current employer, a well-known video game conglomerate, went out of their way to tell us at orientation that they did NOT install trackers, keyloggers, or any such tracking tools for their employees. The fact that they said this, more than once, strikes me as suspicious and HIGHLY unlikely. I don’t understand how they’re able to get away with outright lying to their employees about this.

All of this has a chilling effect on workers’ speech and severely hampers their ability to organize. I am currently part of a labor union that plans to include employee privacy and workplace surveillance in our bargaining contract to protect our rights to a private personal life.
General Comment

I am a freelance software engineer who works by choice as a true independent contractor. Unlike the “independent contractors” misclassified by tech firms like Uber, I work autonomously to achieve goals for clients. They tell me what they want, and I try to deliver it for them on my own time, using my own best judgment. Accordingly, I have never experienced any kind of worker surveillance. While all workers deserve freedom from surveillance, it is especially galling to see independent contractors surveilled. If you need to monitor someone to make sure they’re performing the way you want, they are not an independent contractor. The use of automated surveillance on a worker should be sufficient to disqualify them from being classified as an independent contractor. How can Uber, for example, monitor its drivers through phone accelerometers and GPS[1] while also claiming that they have no say in how drivers are doing the work (the legal definition of an independent contractor[2])?

I also, in my spare time, encourage tech workers to use their protected right to organize. I answer questions about collective organizing and connect workers to labor lawyers and other resources. I have spoken to many remote workers who are scared to speak to their coworkers through digital channels like Slack, Zoom, or email, because they are afraid of being monitored. They lack any other communication channels, and thus have no way of exercising their legal right to organize. Even if these accounts are not being monitored, the workers have no way to be sure of that. It creates a culture of intimidation that can only be remedied by the government stepping in and enforcing monitoring-free spaces for workers.

Despite my privileged position and my personal freedom from worker surveillance, I have seen firsthand the negative impacts of worker surveillance on colleagues and community members. Workers in less privileged positions and facing other forms of marginalization face even more harm from surveillance. I urge the OSTP to ban or limit worker surveillance in order to protect workers from exploitation, the restriction of their fundamental rights, and other kinds of harm.
STOP THE WATCHING; HIRE A SUPERVISORY.
There is considerable evidence that surveillance is biased, because algorithms are biased, because humans are biased (whether or not we are aware of our biases). That alone is a good reason to avoid using it. Beyond that, surveillance is intimidating to workers. I think that for most people it would be nerve wracking and distracting. Inexperienced workers would be afraid that they might make some small mistake and lose their job over it. If you want hard working, dedicated employees, allow them to form unions and provide good pay and benefits.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0024
Comment on FR Doc # 2023-09353

Submitter Information

Name: Kenneth Bryan
Address: United States,

General Comment

Dictatorship
Although I am no longer working, I do eat in restaurants and the very idea that my servers, the bus people etc are being monitored appeals me. Wherever I eat the servers are doing their utmost to care for us as patrons. They do not need to be monitored to improve their “efficiency”! I totally oppose treating people this way, period.
The 21st Century Cares act Federal mandate of Electronic Visit Verification (EVV) for billing for Medicaid waiver services started on January 1, 2021. I am a parent (b) (6) that receives waiver services in our home. We have a caregiver that works with our son in our home and I as a parent also bill for hours under the Indiana State Medicaid waiver. We were told by the provider we use that we had to download an app on our phones or tablets that will require an Electronic visit verification (EVV) log in and log out. This app has GPS and will send where we are at while we are billing for services to a system overseen by the government. I am very concerned about my household's privacy and being tracked by the government. I feel that this a violation of my rights and my son's rights as American citizens. I do believe that services need to be tracked when they are rendered in a group home or at a facility/workshop where there is no parent oversight. But when a beneficiary of a waiver lives at home and services are rendered in home and tracked it is an invasion of privacy and jeopardizes the security of our home and my son's safety.

Maryann Becich
Docket: OSTP-TECH-2023-0004  
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001  
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0027  
Comment on FR Doc # 2023-09353

Submitter Information

Name: Joseph Lawson  
Address: United States,

General Comment

Constant surveillance is a violation of our individual right to privacy and must not be tolerated!
No employer should use workplace surveillance. What is working with these employers not wanting you to have any personal freedoms. This is ridiculous!
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0029
Comment on FR Doc # 2023-09353

Submitter Information

Name: Karen Heesch
Address: United States,

General Comment

Work place surveillance is not in the customer’s best interest.
The rise of automated surveillance and management systems at workplaces has begun to affect the everyday lives of workers across industries, with restaurant workers being significantly impacted. This new technology, although promising in theory, can lead to intrusive monitoring, thereby infringing upon the rights and dignity of workers.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0031
Comment on FR Doc # 2023-09353

Submitter Information

Name: Chas Griffin
Address: United States,

General Comment

?
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0032
Comment on FR Doc # 2023-09353

Submitter Information

Name: Don Pew
Address: United States,

General Comment

Its not good.
General Comment

Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
General Comment

Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0035
Comment on FR Doc # 2023-09353

Submitter Information
Name: CF Massey
Address: United States,

General Comment
WHY ??
NFIB (National Federation of Independent Business) comment letter of June 8, 2023, to the Director of the Office of Science and Technology Policy in response to the notice titled "Request for Information; Automated Worker Surveillance and Management," 88 Fed Reg 27932 (May 3, 2023), is attached.
June 8, 2023

Hon. Arati Prabhakar, Ph.D., Director
Office of Science and Technology Policy
1650 Pennsylvania Ave. NW
Washington, DC 20504-0002

Dear Madam Director:


This letter presents comments of the National Federation of Independent Business (NFIB) in response to the Office of Science and Technology Policy (OSTP) notice titled "Request for Information; Automated Worker Surveillance and Management" and published in the Federal Register of May 3, 2023. The OSTP requested information on the use of automated surveillance and management (ASM) in the workplace, such as to surveil: the location of employees, the pace or quality of the work of employees, communications of employees, interactions of employees with others, and computer activity of employees. Before OSTP immerses itself in the details of use of ASM in the workplace and considers proposals for federal agencies to regulate use of ASM, OSTP should consider what principles will guide its review of the subject of ASM.

NFIB is an incorporated nonprofit association representing small and independent businesses. NFIB protects and advances the ability of Americans to own, operate, and grow their businesses and ensures that the governments of the United States and the fifty states hear the voice of small business as they formulate public policies. NFIB recommends and requests that OSTP adopt the following three principles to guide OSTP's consideration of ASM in the workplace:

1. A business owner has a property right to use ASM to monitor for business purposes, such as safety, security of the premises, and efficiency of the workforce, the business place the owner owns.

2. A business should inform employees and applicants for employment of what use the business makes of ASM, so that they can, by choosing thereafter to work in that workplace, give informed consent to such use of ASM as it affects them in the workplace.
3. Business use of ASM must conform to applicable laws protecting employees, including those protecting highly valued privacy rights (such as prohibitions on monitoring in dressing rooms, restrooms, and locker rooms) and highly valued associational rights (such as the right to engage in concerted action for mutual aid or protection).

Questions concerning ASM in the workplace arise at the intersection of the property rights of business owners and the privacy and statutory rights of employees. OSTP should take care to protect not only the rights of employees, which was the tenor of the request for information that OSTP published, but also should take care to protect the property rights of business owners. Please bear in mind the property rights of business owners, and especially owners of small businesses, as OSTP considers the subject of the use of ASM in the workplace.

Sincerely,

(b) (6)

David S. Addington
Executive Vice President and General Counsel
Workers should not be surveilled! It is NOT 1984!!
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0038
Comment on FR Doc # 2023-09353

Submitter Information

Name: Susan Goldstein
Address: United States,

General Comment

Employees don't deserve being disrespected by being under surveillance.
I am not a restaurant worker, but I deplore the practice of surveillance by employers and managers. This is not how mature adults behave with each other, and it will not improve conditions for workers or service for customers. Restaurant workers deserve to be treated with more dignity, not less.
We need to feel valued.
Table-side tablets erode meaningful customer interactions. The AI restaurant layout manager disregards the human element and disrespects servers' health and safety. Wearable tech for monitoring feels intrusive and surveillance software systems managing shifts disregard servers' personal needs. They need to feel valued, not just efficient. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0042
Comment on FR Doc # 2023-09353

Submitter Information

Name: Peter Reimer
Address: United States,

General Comment

1) ALL employees - from CEO to the lowest paid employee - AT ANY GIVEN company should be EQUALLY surveilled - hour by hour, minute by minute, EQUALLY OR, NONE should be surveilled. 2) ALL surveillance recordings should be equally available, OR, none available for editing, review, etc. 3) should be available to ALL employees at ALL times for free.
Work is stressful and challenging enough with this intrusive, almost-Medieval attitude serfs/oh, no, I mean 21st century workers!
Surveillance creates an atmosphere of mistrust and hatred. Management should strive for building trust with employees and treat them well so they feel a part of the company and behave well. Employees are not slaves or drones and replacing employees with robots kills jobs and kills people. Prevent dystopia now by committing to employing human beings and treating them as such. Where does treatment like animals and automation end? You may be next.
General Comment

While the federal government has legitimate rights to monitor and ensure the accountability of its employees, there should be just as much concern with employees' mental health and welfare when employees have been mandated to excessive workloads in as much as completing the jobs of three individuals. Employees have been mandated to consistently work three jobs after subsequent to being employed without adequate compensation for numerous years. This has been a concern of many employees which has not been resolved nor the employees compensated and now instead of acknowledging those employees the federal government instead seeks the need to further breach trust with surveillance. The perception of being constantly monitored can lead to a further decline in trust between employees and management, fostering a hostile work environment where employees truly feel undervalued, unsupported and misled. Since the pandemic the workload of federal employees have tripled and with unsurmountable issues with fatigue and mental health issues the government now wants seeks information on how to complete surveillance on federal employees with artificial intelligence instead of seeking ways to incorporate AI in the improvement of how services are delivered to the American public and how things could be made more efficient and effective. The regulation of AI should be the most important factor the government should be concerned with regarding AI and all the privacy issues and fraud this could pose.
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information: Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0046
Comment on FR Doc # 2023-09353

Submitter Information

Name: John Ahlquist
Address: [Redacted]
Email: [Redacted]

General Comment

See attached file(s)

Attachments

Surveillance_Comment
New survey evidence shows frontline workers in 5 major industries perceive widespread surveillance aimed at discipline and control.

John S. Ahlquist & Jake Grumbach

Under the auspices of the Worker Empowerment Research Network (WERN)—an interdisciplinary collaboration of scholars and practitioners—we fielded an original survey of 2,561 workers in five select industries known for low wages, scheduling instability, worker churn, and intense recent unionization drives: healthcare, hospitality, retail, telecommunications, and warehousing. Survey interviews took place in the Fall of 2022.

Among other things, we asked workers about their perceptions of whether and why they are surveilled by management with respect to their work productivity, physical location, conversations with coworkers, and phone and computer usage.

We find that over 74% of workers believe they are monitored in some way. A majority believe that their productivity is tracked. 45% report that employers monitor at least one of the following: their location, conversations with coworkers, phone usage, computer usage.

When asked why they believe they are monitored, 57% of respondents “agree” or “strongly agree” that they are monitored for purposes of control or discipline whereas 46% agree or strongly agree that monitoring is for purposes of professional or skill development.

Figure 1 displays reported surveillance rates by industry. Surveillance is generally highest in telecom, retail, and warehousing. Location tracking was most prevalent in warehousing, with nearly 1/3 of warehousing workers reporting location tracking. Tracking of computer usage was highest in telecom (34%) followed by healthcare (25%).

Figure 2 displays workers opinions about why they believe management surveilles them. In general, workers across industries believe they are surveilled for purposes of control and discipline. Workers in telecom and warehousing are more likely than workers in the other industries to report that surveillance on the job is used for development.
Figure 1

**Workplace Monitoring by Industry (Weighted)**

Do you believe you are monitored by your management while you are at work in your primary job? Yes, my employer monitor my...

![Bar chart showing workplace monitoring by industry](chart1.png)

*Note: Respondent can select more than one option.*

Figure 2

**Monitoring Used to ... by Industry**

Develop workers' skills and abilities or control and discipline workers.

![Bar chart showing monitoring by industry](chart2.png)

*Note: Respondents are only shown the question if they are monitored for productivity (Q4.8: surveillance_productivity).*
I have worked remotely for nearly a decade here in the U.S., for multiple companies (including UBM, Informa, and Future US), and I can say unequivocally that any additional monitoring or surveillance of my activity during the work day would be detrimental to my wellbeing without any meaningful improvement in my productivity. I know this because I have been part of several attempts to institute systems of automated worker management and surveillance in the workplace, (due to added stress, added work that is not being done in the name of the business but rather in the name of verifying productivity, thus wasting time that could be spent on work that furthers the business) and led to greater employee unhappiness and departure rates.

Frankly, the only reason I've ever seen anyone stay employed at a business that uses automated worker surveillance and management tools is because they can't afford to quit. Using "productivity-enhancing" tools which literally make people want to leave, and only stay if they *have no other employment options* available to them, is a clear example of employer overreach predicated on taking advantage of people who don't have better opportunities. Thus, I humbly and strongly beg regulators to put laws in place which protect workers and prevent greedy employers from using new technologies to wring more "value" out of workers who have no power to stop them.
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information; Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0048
Comment on FR Doc # 2023-09353

Submitter Information

Name: Kate Bronfenbrenner
Address:
Email: [REDACTED]
Phone: [REDACTED]

General Comment

See attached file(s)

Attachments

whitehouse_surveillKB
Surveillance during NLRB Certification Elections
Kate Bronfenbrenner,

In 2022, we conducted an in-depth study of employer opposition in NLRB certification elections, updating findings from the series of studies on NLRB campaigns we had conducted since 1988. Lead organizers were surveyed in a random sample of 533 NLRB certification elections held between January 1, 2016-June 30, 2021, with a response rate of 56 percent (297 cases). We also supplemented our research with a review of all unfair labor practices filed during the election campaigns in our sample. We found that employer use of surveillance more than doubled in the last twenty years, going from 14 percent to 35 percent of all NLRB elections and 40 percent of elections where the employer mounted a campaign.

<table>
<thead>
<tr>
<th>Table 6(b) Employer opposition and election outcome: Surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>All NLRB Elections</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>1999-2003</td>
</tr>
<tr>
<td>Proportion of elections</td>
</tr>
<tr>
<td>Win Rate*</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>All types of surveillance</td>
</tr>
<tr>
<td>Surveilled workers’ social media</td>
</tr>
<tr>
<td>Surveilled workers’ phones and key cards</td>
</tr>
<tr>
<td>Surveilled workers using cameras</td>
</tr>
<tr>
<td>Used electronic surveillance</td>
</tr>
<tr>
<td>Employee key cards</td>
</tr>
<tr>
<td>Employee ID badges</td>
</tr>
<tr>
<td>Employee phones or app technologies</td>
</tr>
<tr>
<td>Computer log-in authentication</td>
</tr>
<tr>
<td>Employer computer or phones</td>
</tr>
<tr>
<td>Searches upon exits and entry</td>
</tr>
<tr>
<td>Worker footsteps or movements</td>
</tr>
<tr>
<td>Wearable devices that monitor speed</td>
</tr>
<tr>
<td>GPS technology that monitors location</td>
</tr>
</tbody>
</table>

The increase in workplace surveillance is likely a consequence of developments in electronic surveillance and the widespread use of social media. Fourteen percent of employers who mounted campaigns surveilled social media, and 20 percent used cameras to spy on their
employees. Twelve percent used a combination of electronic surveillance techniques such as employee key cards, ID badges, phone and computer apps, GPS location devices, and tracking of movements, speed, and exit and entry.

Given the ability of firms to use surveillance without the knowledge of workers or the union, it is likely that these statistics greatly undercount the use of surveillance during NLRB certification election campaigns. Campaign win rates drop from 73 percent to 62 percent when the employer uses surveillance. First contract rates fall from 58 percent to 38 percent. When included in logistic regression analysis, controlling for election environment, bargaining unit demographics and employer and union characteristics and tactics; surveillance is negatively and significantly associated with percent union vote and win.

Surveillance for union activity is a serious labor law violation, yet, as an 8(a)1 violation of the National Labor Relations Act, there are no financial or punitive penalties against employers who surveill workers during organizing campaigns. Until this changes, employers will continue to actively and illegally interfere with workers rights to organize and bargain collectively.
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0049
Comment on FR Doc # 2023-09353

Submitter Information

Name: Merve Hickok
Address:

Email: [REDACTED]

General Comment

Please see attached our recently published Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools. Since this work addresses many of the questions of RFI, I am submitting in full.

The Policy Primer analyzes the impact of these technologies on human and worker rights, human dignity, role of unions, fair and equitable work places.

The Roadmap provides policy recommendations for federal government legislation, agency enforcement actions (EEOC, FTC, NLRB), as well as recommendations for labor unions.

Merve Hickok [REDACTED]

Attachments

A policy primer and roadmap on AI worker surveillance
A policy primer and roadmap on AI worker surveillance and productivity scoring tools

Merve Hickok1 · Nestor Maslej2

Received: 2 March 2023 / Accepted: 7 March 2023 © The Author(s), under exclusive licence to Springer Nature Switzerland AG 2023

Abstract

Algorithmic worker surveillance and productivity scoring tools powered by artificial intelligence (AI) are becoming prevalent and ubiquitous technologies in the workplace. These tools are applied across white and blue-collar jobs, and gig economy roles. In the absence of legal protections, and strong collective action capabilities, workers are in an imbalanced power position to challenge the practices of employers using these tools. Use of such tools undermines human dignity and human rights. These tools are also built on fundamentally erroneous assumptions. The primer section of this paper provides stakeholders (policymakers, advocates, workers, and unions) with insights into assumptions embedded in workplace surveillance and scoring technologies, how employers use these systems which impact human rights. The roadmap section lays out actionable recommendations for policy and regulatory changes which can be enacted by federal agencies and labor unions. The paper uses major policy frameworks developed or supported by the United States as the foundation for policy recommendations. These are Universal Declaration of Human Rights, the Organisation for Economic Co-operation and Development (OECD) Principles for the Responsible Stewardship of Trustworthy AI (OECD AI Principles), Fair Information Practices (FIPs) and the White House Blueprint for an AI Bill of Rights.

Keywords Algorithmic surveillance · AI surveillance · AI governance · Human rights · Worker rights · AI bias

1 Introduction

The surveillance of workers and the obsession with tracking worker behavior as a means to measure productivity are not new phenomena. However, effective policy implementation and regulatory interventions for these practices are either non-existent or minimal. Some policy frameworks demand products and services to be “lawful.” However, when no law or oversight exists to protect workers against the surveillance and productivity scoring technologies, workplaces are turned “into sites of experimentation with these systems” [1].

Increasing data collection and use of artificial intelligence (AI) technologies in the workplace affects all industries. This Policy Primer and Roadmap focuses on workplace surveillance and productivity scoring tools and practices. In two sections, the Primer provides a range of stakeholders—workers, policymakers, unions, employers and vendors—with insights into these technologies, and the Roadmap lays out actionable recommendations for change.

In the following sections, the stakeholders can find:

- An overview of worker surveillance and productivity scoring tools in the market, and the adoption trends by employers.
- A brief history on similar employer practices; of worker surveillance and productivity scoring.
- Insights on how human rights can be undermined, and how workers’ access to resources and opportunities can be limited by deployment of these tools, and
- The erroneous assumptions made about these tools.
- The final part provides a roadmap for stakeholders, and possibilities for different policies to be adopted.

The analysis brings together several major policy frameworks which should guide policy and regulatory decisions,
especially in the United States. These are the Universal Declaration of Human Rights (UDHR) [2], the Organisation for Economic Co-operation and Development (OECD) Principles for the Responsible Stewardship of Trustworthy AI (OECD AI Principles) [3], Fair Information Practices (FIPs) and the Blueprint for an AI Bill of Rights (Blueprint) [4].

The United Nations unanimously adopted the UDHR, recognizing all individuals are entitled to inherent, inalienable set of rights. The document was drafted by a committee chaired by Eleanor Roosevelt and adopted in the General Assembly meeting in 1948.

In late 2022, the White House Office of Science and Technology announced the Blueprint which focuses on “use of surveillance technologies when juxtaposed with real-time or subsequent automated analysis and when such systems have a potential for meaningful impact on individuals’ or communities’ rights, opportunities, or access” and hence having a major impact on human rights. The Blueprint defines these technologies as “products or services marketed for or that can be lawfully used to detect, monitor, intercept, collect, exploit, preserve, protect, transmit, and/or retain data, identifying information, or communications concerning individuals or groups” [5]. The Blueprint also draws a parallel to 1973 report Records, Computers, and the Rights of Citizens [6].

Allen and Rotenberg summarize the origins of FIPs as “Fair Information Practices were first articulated in the United States Department of Health, Education and Welfare’s seminal 1973 report Records, Computers, and the Rights of Citizens [6]. Computer scientist Willis Ware was the chair of the Advisory Group responsible for the report and is credited with the creation of the phrase “fair information practices.” The framework was immediately influential, as it provided the basis for the federal Privacy Act the following year. In most simple terms, Fair Information Practices allocate rights and responsibilities in the collection and use of personal information. Organizations that collect and use personal information take on the responsibilities, while individuals whose personal information is acquired obtain the rights. Most modern privacy law follows this structure” [7]. In the legislative process, Congress concluded the Privacy Act with eight principles: Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual Participation, and Accountability [8].

The United States contributed significantly to the development of OECD AI Principles announced in 2019 (which were subsequently also adopted as G20 Principles), and which are now endorsed by more than fifty countries. These principles include inclusive growth, sustainable development and wellbeing; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability.

As a major policy document from the executive branch, the Blueprint brings fundamental rights and democratic values to the forefront of how we should evaluate technology and its impacts. Blueprint also highlights the importance of OECD AI Principles and FIPs. The Blueprint is a product of collaboration by different departments of the federal government. The document lays out five principles crucial to the protection of rights and democratic values. One can read the Blueprint as a call to workers:

- **Safe and effective systems**: You should be protected from unsafe or ineffective systems. This includes protecting you from foreseeable harms from uses or impacts of automated systems.
- **Algorithmic discrimination protections**: You should not face discrimination by algorithms and systems should be used and designed in an equitable way.
- **Data privacy**: You should be protected from abusive data practices with built-in protections, and you should have choices over how data about you is used.
- **Notice and explanation**: You should know an automated system is being used and understand how it can impact you.
- **Human alternatives, consideration and fallback**: You should have access to appropriate human alternatives and other remedies for systems resulting in discrimination or other harms.

### 2 The primer

#### 2.1 Overview

Digital worker surveillance refers to the use of digital tools to monitor worker activity. There are a variety of tools employers use to conduct such surveillance. In recent years databases have been released tracking the use cases for various kinds of new labor technology tools, including ones for worker surveillance and productivity improvement [9, 10]. To gain a fuller picture of what modern workplace surveillance entails, it is worth exploring three examples of such surveillance in further detail. Prodoscore is a worker monitoring software which deploys a proprietary algorithm to assign workers a daily productivity score out of 100 [11]. More specifically, Prodoscore considers various inputs such as emails sent, phone calls made, messages on company messaging apps and activity on databases. The scores are then released to managers and furthermore ranked, meaning that the managers can assess how the productivity of various workers stack up against others [12]. Another surveillance software, RemoteDesk uses facial recognition technology to monitor workers who handle sensitive information in their jobs. Such a system might be deployed for example,
for workers who frequently see credit card information [13]. If the system detects that someone else is looking at the screen while a credit card is being displayed or if there is a recording device in view, it will send an alert. However, this very system can also send alerts if workers work or eat on the job. Workers delivering goods or food, workers at warehouse workstations, or those moving around within a building (such as construction or housekeeping workers) can all be subject to different kinds of surveillance. Another example is UPS retrofitting its delivery trucks with multiple sensors to track the break times drivers were taking and further facilitate the optimization of deliveries [14]. As a result of installing these sensors, UPS was able to increase the total number of packages it was delivering per day, while requiring significantly fewer drivers.

The rise of surveillance technologies has been accompanied by a growing consciousness surrounding the pervasiveness of such tools. In an era of smart devices and sensors all around us, the estimate on prevalence of worker surveillance technologies vary. However, all the available estimates make it clear that the adoption of these technologies are rapidly increasing. For instance,

- A 2022 New York Times article found 8 out of 10 of America’s largest private employers use some kind of productivity tracking tools [15].
- A study commissioned by ExpressVPN, in collaboration with Pollfish, surveyed 2000 employers and 2000 employees who work in a remote or hybrid capacity. 78% of employers reported using employee monitoring software to track employee performance and/or online activity [16].
- Gartner research shows the number of large employers using worker tracking tools has doubled since the beginning of the pandemic to 60%, with this number expected to rise to 70% within the next three years [17].
- The Wall Street Journal reported on a 2022 survey conducted by the research group International Data Corp which found 67% of North American employers with at least 500 employees deploy employee monitoring software [18].
- Zety study on workplace surveillance shows 85% employers use workplace surveillance [19].
- Top 10 VPN report shows global demand for employee surveillance software increased by 78% in January 2022 [20].
- Digital.com survey found 60% of companies employing remote workers use tracking software. This survey released in January of 2022 polled 1250 US employers on their use of surveillance technologies [21]. Moreover, 88% of companies terminated workers after implementing the surveillance software. This survey also sheds light on the particular kinds of tracking functions these employers are deploying: 76% use tools to track web browsing and application use, 60% capture random screenshots, 54% block specific content and 44% track keystrokes. However, the rate of usage varies by industry and is perhaps unsurprisingly the highest in either low-wage industrial settings or in employment relationships with billable hour work models, such as advertising and marketing (83% of companies reported using surveillance tools), construction (71%) and business and finance (60%).

Employers provide a wide range of justifications for surveillance technologies, most of which center around better control of workers and improving productivity. For example, employers claim the surveillance and productivity scoring tools are essential in enabling them to identify both productive and unproductive workers [15]. Again, the Digital.com survey is helpful in accessing employer motivations. When asked why they use surveillance software the top reasons employers provided concerned understanding how workers use their time (79%), confirming that workers are working full days (65%) and ensuring that work equipment is not being used for personal use (50%) [21].

### 2.2 History of worker surveillance

Employers have been interested in surveilling and improving worker productivity since arguably the beginning of the market revolution. The market revolution which began in the early nineteenth century was a pivotal moment in industrial history, as it was one of the first times when an increasing number of Americans went to work in factories for employers. Work in factories governed by shifts, production quotas and clocks is fundamentally more regimented and controlled than the work Americans were previously doing on farms or in trade shops. Many historians have argued this period bore witness to some of the most fundamental changes in US history [22].

When factory work became much more firmly established, employers were interested in more pointed questions about how to heighten productivity through closely tracking worker activity. “The marriage between work, the hour, and pay became standard within the factory” [23]. Individuals like Frederick Winslow Taylor, one of the world’s first management consultants, authored The Principles of Scientific Management and laid out a precise vision for ways workers could be better managed, monitored and controlled for the sake of improving productivity [24]. There are likewise anecdotes from this era, of Henry Ford pacing on factory floors with a stopwatch to push worker efficiency, or hiring private investigators to gain a sense of how the personal lives of his workers could potentially impede productivity [14].
The desire on behalf of employers of tracking for the sake of productivity is not unique to the twenty-first century. However, it is necessary to note the development of new technologies has made the task of surveillance much more possible than it once was. After all, there is a natural upper limit to the human capital any company can deploy for the purposes of supervision. Returning to the example of Henry Ford, there can only be so many factory-floor managers or private investigators hired and deployed. New technologies, however, make it both easier and more cost effective to track workers. Cameras and sensors can be installed practically anywhere. Other connected devices (such as smartphones, wearables, laptops, etc.) necessary to conduct work can be simultaneously used as surveillance devices.

Two additional trends have further heightened the use of surveillance tools. First, in the last couple of decades an increasing number of Americans started telecommuting or working remotely. For instance, from 2005 to 2012, 79% more American workers started telecommuting [14]. Increasing number of online platforms and applications also gave rise to gig workers. This number of course then skyrocketed as a result of the COVID-19 pandemic [25]. During the pandemic many employers pivoted towards remote work. Even as the pandemic controls ease, remote work or hybrid arrangements continue as common practices. Given that less workers are now working in actual offices, companies doubled down on surveillance tools as a means of regaining the control they once maintained in the office.

3 Worker surveillance, productivity scoring and impact on fundamental rights

Developers of AI and algorithmic systems promise these systems benefit organizations by increasing the efficiency, effectiveness, and scalability of processes, “streamlining and redefining” the workplace, reducing costs and standardizing application of rules—and hence improve profitability [15]. However, there is also a group of AI applications available in the market, which promise employers different capabilities to track, monitor and assess their workers. The power to have an all-seeing eye over the workforce is attractive to many employers. These technologies were once more prevalent in factory settings. The gaze of algorithmic surveillance was and is still disproportionately on low-income workers., The workers are now spread across different work contexts such as logistics, hospitality, food and service delivery jobs, or gig workers in online platform companies [26]. These jobs are then disproportionately held by workers of color. However, the reduced costs and improved capabilities for data collection, processing and retention also allows surveillance to extend to pink- and white-collar workers too. Worker surveillance is becoming a common phenomenon across all workplaces. When surveillance moves from the factory or warehouse floor to the devices workers use from other settings (such as home office, vehicles) or even carry on their bodies, surveillance becomes inseparable—it also ‘bleeds into’ workers’ private lives [11, 14]. As these workers become hyper visible through surveillance systems, the employers become more invisible behind the algorithmic decision-making systems.

3.1 Worker surveillance

It is easier to notice the physical cameras around us. However, with surveillance technology available in many shapes and forms, it is not always easy for the workers to know they are being monitored, and their data is collected. In the US, Employers can use such tools without informing their workers [27]. Workplace data collection powering surveillance can be achieved by a combination of hardware and software as listed below.

<table>
<thead>
<tr>
<th>Hardware and software</th>
<th>Analysis</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing (laptop, tablets)</td>
<td>Productivity tracking</td>
<td>Outputs (tasks/items/transactions/sales completed)</td>
</tr>
<tr>
<td>Smart phones</td>
<td>Risk assessment</td>
<td>Communication (Email, text, chat, voice, collaboration tools)</td>
</tr>
<tr>
<td>Wearables (fitness tracker, smart watch, body cam)</td>
<td>Culture fit</td>
<td>Social (posts, comments, likes, 3rd party social media backgrounds checks)</td>
</tr>
<tr>
<td>IoTs (RFID sensors, thermal imaging, counters, WiFi routers, GPS)</td>
<td>Count of outputs</td>
<td>Engagement (calendar activity, Time spent online)</td>
</tr>
<tr>
<td>ID badges (fitted with microphone and accelerometer)</td>
<td>Workplace analytics</td>
<td>Search history (browser search terms, website visited)</td>
</tr>
<tr>
<td>Camera (CCTV, laptop camera activation)</td>
<td>Insider threat</td>
<td>Location (access management, geolocation tracking, geofencing)</td>
</tr>
<tr>
<td>Screen capture</td>
<td>Biometric ID verification for shift/ workplace access</td>
<td>Fitness (activity, prescriptions)</td>
</tr>
<tr>
<td>Keystroke logging</td>
<td></td>
<td>Login (user ID and password capture)</td>
</tr>
<tr>
<td>Call recording</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice assistant recording</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric recognition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2 Productivity scoring

“All things that can be counted counts. And not everything that counts can be counted.”—paraphrased from William Bruce Cameron [28].

The attraction of new technologies and vendor claims to extract actionable ‘productivity’, ‘risk’ or ‘fit’ scores for workers give rise to a variety of black-box algorithmic
products in the market [29]. The products collect a plethora of data points and compare them against subjective rules to provide a score for a worker or infer certain behavioral characteristics. These scores can then be used by human managers to make determinations about the workers efficiency, productivity, risk to company’s assets and reputation. The scores also drive decisions about wages, benefits, promotions, disciplinary action or even terminations. At the extremes, these decisions can be automated and do not even require a human manager to review and validate.

When one thinks of how surveillance and scoring systems work, and how they are connected, it might be helpful to break the process down into smaller components. First, a method to track and record worker activity is necessary. Hardware, such as company-provided devices (phone, tablet, wearable fitness trackers), camera, wireless connection routers, sensors can be used to collect raw data on worker communications, online activity, movement, work outputs etc. Then, once the data is collected, an algorithmic model is necessary to analyze the collected data and make inferences or determinations about the worker behavior and performance. Developers make various design decisions on how to collect data and how to build these AI models. At times, there might be legitimate reasons to install certain data collection technology to ensure workers safety and security. Alternatively, the employer might be required by law to record worker communications. However, outside of these very limited reasons, most of these technologies are built upon problematic design decisions. The choice of the term ‘surveillance’ over ‘monitoring’ in this paper is intentional. Surveillance acknowledges the power employers hold over workers and the practices of ubiquitous collection of data on worker communications, engagement and interactions used mainly for the benefit of the employer. The data can then be used in control and manipulation of work engagement and contractual negotiations (if a contract even exists).

Vendors of these scoring systems claim the surveillance data collected can be used to infer the productivity, risk or fit of workers in relation to their roles. The claims and embedded design decisions include fundamentally erroneous assumptions, such as the ability for technology to correctly capture a human’s complex nature, or infer emotions and sentiments, or that human behavior can always be predicted. Use of surveillance and scoring technologies also infringe upon an individual’s rights and freedoms. These technologies and assumptions embedded in them can be in direct contradiction with fundamental human rights [4]. Despite the impossibility of delivering on their marketing promises, these systems still find buyers among the business decision-makers.

**Human dignity:** Surveillance first and foremost degrades human dignity. Even if workers know about surveillance technologies, they may not have the possibility or privilege of leaving a job due to concerns over aggressive data collection or algorithmic decisions. If worker consent is requested at all, workers are asked to choose between their ability to earn a wage versus their data being collected. Their choice naturally favors employment. In such an imbalanced power situation between employer and worker, one cannot count the consent as a free or informed one. The workers lose control of privacy over their own bodies, movements, and even social interactions [30]. Who gets to draw the boundary about what is crucial information for an employer? In the absence of protections by law or organized labor, the workers are left to themselves to defend against surveillance. The boundary line is drawn ‘upon’ their bodies.

Human dignity is undermined again in the scoring systems as human complexity, engagements, aspirations, and creativity are reduced to points of data and spurious correlations. There is no longer a human story behind the interaction, nor is there the ability to ‘bring your whole self to work.’ The essence of the worker and complexity of a being and human interactions are boiled down to the data deemed important by vendors and employers, and data which can be collected.

Legal scholar Ifeoma Ajunwa also highlights that especially wearable data collection technologies may create new legal challenges such as the possibility that employer engages in unlawful surveillance (defined under National Labor Relations Act) “when it surveils employees engaged in concerted activities by observing them in a way that is ‘out of the ordinary’ and therefore coercive [31]” Such practices also undermine fundamental principles such as the Fair Information Practices, which include collection limitation, purpose specification, use limitation, accountability, security, notice, choice, and data minimization [32]. For example, data initially collected by third parties (such as fitness trackers provided by wellness or insurance companies) via the employers, can eventually be used in ways that restrict the worker’s access to resources and opportunities elsewhere [14].

**Right to privacy:** One of the most cited issues in worker surveillance is the infringement of privacy. The right to privacy is considered a fundamental human right. In the United Kingdom, Barclays bank faces a $1.1 billion fine over alleged monitoring of employees [33]. In Germany, data protection regulator fined electronics retailer notebooksbilliger. de for $12.6 million for using video cameras to surveil workers [34]. However, in the US, employers can collect information when workers use organization-provided devices or networks. In the absence of federal privacy regulations, a privacy regulator, or any laws limiting worker surveillance practices, the status quo allows employers to do as they see fit for their own interests. However, legal does not always mean ethical.
A recent OECD working paper AI in the workplace highlights that use of AI systems can “extend and systematize ethical failings and fundamentally change the relationship between workers and their managers” [35]. Some surveillance practices cross the line between work and private life where employers can capture very private information about the workers. For example, employers can engage in (1) social media surveillance, (2) video surveillance in the office, (3) mandate workers to use smart assistants which record conversations, or leave their laptop cameras on, (4) take screenshots of monitors at random times during the day, or (5) force workers to download mobile applications on their personal phones which continue to collect information outside of working hours. In 2022, a Dutch court ruled an employer requiring employees to keep webcams on for several hours a day and share screens, violated the right to respect for private and family life. In Germany, the data protection regulator fined retail company H&M for $41 million for the illegal surveillance of employees and keeping “excessive” records on the families, religions and illnesses of its workforce [36]. The European Court of Human Rights had a similar ruling in 2017 [37]. Such intrusion can also lead to unintentional disclosure of information protected by Title VII of the Civil Rights Act of 1964 [38] (such as sex, race, color, national origin or religion, sexual orientation, etc.) or Americans with Disabilities Act (“ADA”). Although non-discrimination regulation prevents employers from making employment decisions based on this protected information, knowledge of such information can lead to possible unconscious biases nevertheless [26, 39]. The target of surveillance shifts from the work to the worker. Notice of such protected information which would not otherwise have been known to the employer can create legal risks for the employer and opens the possibility for allegations of discrimination [40].

**Right to expression:** Ability to surveil a worker’s private and social interactions undermines freedom of expression. By monitoring emails, chats, phone conversations, employers can get access to workers’ thoughts—without discriminating between personal and professional communications. Knowledge of surveillance can force workers to self-filter or self-regulate their expressions and ideas. In parrothing Foucault’s “technologies of the self”, Manokha highlights the power of surveillance on individuals to self-restraint and self-discipline [41]. In this case, workers, aware of being under surveillance, may end up self-restraining themselves without any coercion or use of force by employers [42]. Employers’ interest in surveilling communication also spills over to personal lives. More and more companies are interested in worker or job applicant social media accounts [43], and some even have patented audio technology to eavesdrop on conversations among workers and customers [44]. Some companies demand login access to social media accounts to enable surveillance of these accounts. In certain states where this boundary is protected by law, employers are able to continue the practice via third-party vendors. These vendors parse social media presence and interactions of both candidates and workers and provide ad hoc or ongoing risk scoring to employers. Risk scoring models can create spurious correlations, however many employers still use outcomes as third-party assessment for their employment decisions. Knowing employers can see and act upon their social media posts can prevent workers from expressing their true identities (i.e. sexual preference, religion, ability, etc.) outside of the workplace. Workers can also refrain from posting about social, economic, political, or other societal issues. This can eventually result in significant societal impacts.

**Right to data protection:** The data collection enabled by AI surveillance technologies is ubiquitous and pervasive. Without federal privacy legislation or robust worker protections, employers not only collect data but can also share the data further with third parties for different purposes. Workers may not access data collected about them or have any say over what the collecting entity might do with their data. Most of the time the workers may not even understand the full complexity of the data, the inferences made about them, or the extent of possible impact or harm. Both UC Berkeley Center for Labor Research and Education [1] and CoWorker.org’s [45] studies state that such data collection lacks clear and consistent safeguards. A possible breach of data can impact the worker’s access to benefits, resources and opportunities outside of the workplace.

**Right to collective action and power:** The nature of surveillance creates one party which makes the decision to surveil, collect data and benefit from its conclusions; and another party which gets impacted by the decision. When workers try to reduce the power imbalance through individual resistance or collective action, the data can also be used to oppress protected collective activity such as unionization or grievance. In other words, workers without protection “lack bargaining power to sufficiently fight invasive forms of surveillance, and surveillance is even being used to deter and prevent unionization [46]”.

History offers many examples of corporations hiring private investigators to surveil activities of workers to prevent collective action and break strikes [47]. A 1987 report by the United States Office of Technology Assessment, titled “The Electronic Supervisor: New Technology, New Tensions” provides a historical landscape analysis of tensions and considerations created by electronic employer surveillance systems. The report lists main concerns as privacy, fairness, and quality of work life. The factors included in fairness are listed as “reasonable standards, understanding by workers of the extent and use of the monitoring system, ability of workers to contest or correct records, and participation by workers in the design of the system.” The report makes clear
there are no legal requirements in U.S. law that surveillance be “fair,” jobs be well-designed or employees be reconsulted about work standards, except insofar as these points are addressed in union contracts [48].” The report acknowledges both the low levels of unionization in the United States and how the surveillance issue has created more motivation for collective action in some previously unorganized firms.

Unfortunately, 35 years after this report, unionization rates are lower than 1987 rates, technology allows for more invasive data collection, and unions’ internal capabilities to counter these surveillance practices leave much to be desired. With the ability to collect information ubiquitously, employers can use the emerging technologies to exert power over workers. With such information disadvantage, algorithms “act as a force-multiplier for the power held by firms, with no balancing agent on the side of workers” [49].” In 2021, Spain passed a law requiring online delivery platforms to inform labor unions of how algorithms affect workers’ working conditions [50].

Employers are obliged to “file ‘Surveillance Reports’ to report certain expenditures and arrangements they make in connection with labor disputes [51, 52].” The expenditures clearly include surveillance technologies and activities. However, when workers and unions are rarely aware of covert surveillance practices, it is hard to keep employers accountable for their transparency obligations or challenge fair practices. Scholars Pasquale and Citron advise “secrecy is a discriminator’s best friend: unknown unfairness can never be challenged, let alone corrected [53]. Establishing workers’ data rights under collective agreements not only protects the workers, but prevents the power of unions from diminishing [54].

Right to work and right to just and favorable remuneration: As per the Universal Declaration of Human Rights, every person has the right to work, to just and favorable conditions of work, to equal pay for equal work, and everyone who works has the right to just and favorable remuneration ensuring for themselves and their family an existence worthy of human dignity [4].

Emerging AI technologies increasingly allow previously disparate data to be connected. A great investigative journalism article by ProPublica details how a software sold to landlords can provide them with information regarding the levels of occupancy, rent amounts in their area, and the possibility to communicate with each other over the platform [55]. Whereas previously landlords had to invest significant resources to collect this kind of data individually, such platforms or technological tools now continuously allow the users access up-to-date information. Access to such information can be used to reduce competition and manage vacancies in a way to drive rent prices up beyond their market values. A parallel can be drawn here for wages and worker rights. Tools like Argyle provide aggregated workforce financial data to employers through applicant tracking systems, and to insurance providers, lenders, and credit card issuers through a single API [56]. Argyle’s vision is not only to provide financial data but “holistic view of a worker’s identity including typical hours, work trajectory, reputation and more [57].” In other words, a consolidated way for employers to see a candidate’s employment history and other compensation details before they make an offer. The asymmetrical information power means an employer can offer a less than fair wage rate or cooperate with other employers to suppress wages. Argyle claims to have profiles for more than 175 million workers, covering 80% of the US workforce [56]. While the vendor positions itself as a “third-party verification service which ‘allows’ workers to securely share their income, job title, and proof of employment information with lenders, background check companies, human resources, or any other party they choose [56]” vendor mentions nothing of massive data collection, use and future risks for workers. Some workers may become permanently locked out of employment opportunities due to the recommendations of the systems used by many employers in the industry.

When algorithmic systems become connected to each other for inputs, or the use of the aggregated systems becomes more prevalent in pre-employment decisions, a separate risk emerges. A biased, erroneous or manipulated outcome from one system becomes a direct input to another decision-making system. With such interconnected systems, workers may be locked out of affordable housing, insurance, healthcare, and similar systems [58].

Validity and black-box decisions: Vendors developing the scoring algorithms tend to make a lot of promises about the capacity of their products without disclosing how the scores are calculated, or what design decisions are made within the system. If a client demands to know the science behind the system, the house of cards may fall apart. Instead, it is a lot easier for a vendor to hide behind intellectual property (IP) protections or suggest one should trust the “neutral” technology. However, lack of vetting can expose the employer clients to liability [40]. A client should and can demand transparency. Unfortunately, since both vendors and employers benefit from these technologies in different ways, questions of scientific validity, or whether they should exist in the first place are not of priority.

Even when an employer is aware of the fact the technology is not delivering on the promise, it might still continue with the practice because it at least gives it a way to collect information about worker activity. The employer may choose to fix the issue with another level of surveillance. For example, when an AI system tracking the movements of workers in an Amazon warehouse fails, video footage is sent to other workers in India and Costa Rica. These workers provide input to improve Amazon’s machine learning tools’ accuracy for surveillance. The workers have “no idea where
this particular data [is] going...and what exactly is happening in the backend.” These remote workers were also not aware that they themselves were being monitored by screen and mouse activity [59].

**Right to due process:** “Data-centric technologies hide, obscure, and validate employer behaviors behind an algorithm [60, 61].” Scoring can lead to automatic penalties in wages, shift distributions, and sometimes even to loss of job [15]. Without understanding how the surveillance and productivity scoring algorithms are used to make determinations about their wages, benefits or work conditions, or the unions putting in safeguards in contract clauses, “workers have few pathways to contest harmful employer decisions like discrimination and wage theft [62].” In many jurisdictions, workers also face the additional challenge of algorithms protected by intellectual property legislation. This means that even if they have the means to analyze algorithmic models, workers or unions may still not have access to them. Workers surveilled and scored by these algorithms need enhanced rights—such as right to procedural data due process [63]. In the US, ‘at will’ employment arrangements, used in most low-income jobs, allow both employers and workers to terminate the relationship at any time without having to provide a reason. However, many other employment decisions could still benefit from due process requirements.

**Normative judgements:** When the scoring models are created, developers make certain decisions. The decisions can include what activity to collect data on, or in other words, what behavior or activity should count towards productivity or risk. Developers make these decisions based on the technical possibility of collecting a particular set of data and what data should be accepted as a proxy to productive work. They make normative determinations about what ‘normal’ or ‘typical’ productivity should look like, then compare the data collected by workers against those norms. They decide on the labels and categorize workers into these labels. In reducing humans into standard categories, the developers also dehumanize and depersonalize the workers [64]. In making these decisions, developers also embed their own values, experiences, culture and biases into the algorithms they develop [65]. A recent New York Times article on worker productivity tracking articulates this issue as “the working world’s new clocks are just wrong: inept at capturing offline activity, unreliable at assessing hard-to-quantify tasks and prone to undermining the work itself [15].” The “choices in which factors to prioritize, or their failure to specify all relevant factors, can result in unanticipated consequences [102].”

By measuring everyone against a certain norm, and requiring similar behavior, these algorithmic systems create homogeneity. Charlie Munger, vice chairman of Berkshire Hathaway, one of the most successful business investors says, “Mimicking the herd invites regression to the mean (merely average performance) [66].” Companies globally spend significant amounts of time and resources to attract candidates with diverse backgrounds, experiences, identities and perspectives. When surveillance and scoring systems are used to determine a worker’s conformity to certain norms and behaviors, and discourage differences, the employers end up sabotaging their own efforts in the long run.

**Context and cultural specificity:** Just as the developers of algorithms embed their own normative judgements into scoring systems, they also claim the universality of their products. However, anyone who has traveled to different parts of a country or internationally, would attest cultural differences find their correspondence in work relations. Different cultures prioritize different behavior at work and have variety in how workers interact between themselves.

Even within a homogeneous work environment, scoring systems still cannot capture the complexity of work, nor do they take into account the external factors or circumstances which might be impacting a worker’s ability to deliver an output or complete a task within a certain amount of time. Without appreciating the context of worker interactions and the totality of the effort which goes into creating an output, these systems prioritize quantity and quantification [63] over quality and depth of work. Data is not independent from its context. Some workers subject to productivity algorithms characterize the situation as “infuriating”, “soul crushing” and a “kick in the teeth” as the employers had failed to grasp the totality of the tasks making up their job [11]. The expectation from employers is for workers to be robot-like subjects. This approach leaves no room for differences and diversity, and no appreciation for offline work such as thinking, reading printed material, brainstorming with co-workers, mentoring other workers.

**Disability discrimination:** When these systems make judgements about what be considered typical or expected productivity, they can also lead to other harms for people with disabilities. Some assessments of ADA [39] suggest “If an employer adopts a faster pace-of-work standard and enforces it rigidly, it could run afoul of the ADA’s prohibition against “standards, criteria, or methods of administration... that have the effect of discrimination on the basis of disability [67].” More than half of disabilities are invisible, and are highly diverse, making them “virtually impossible to analyze at scale [68].” In addition, only 21% of employees with disabilities disclose them to their employers’ human resources departments [69]. Access to biometric or health data collected by wearables or via a worker’s social media accounts can give managers or employers additional information to infer ability or health condition of workers, leading to possible biased decisions, or spurious inferences. Even if the information did not play a role in an adverse
employment decision, employers could be alleged to have discriminated due to a disability or perceived disability [40].

The technical shortcomings of the AI system, such as inaccuracies of devices, can also cause unintended harm. For example, wearables collecting health and wellness information may not be accurate in the first place [70, 71] but can be still used for work-related determinations. Since scientific validity of the system and possible technical biases are not questioned, the workers can be subjected to discriminatory outcomes. Or imagine a scenario when the developer, or employer is not aware of the bias in the system. For example, assistive devices (for example screen readers) may interfere with the accuracy of data collected. Or if the scoring systems disadvantage neurodiverse people, those with slower reading speeds or those multitasking, then the outcomes might be discriminatory.

Erosion of trust: The history of worker surveillance provides ample evidence for how employers choose the easier route of surveilling workers rather than investing in establishing trust and a shared vision with their workers [72]. In many cases, employers choose the top-down, hierarchical methods to control and shape. The alternative is co-creation and determination of shared values and vision. Workers trusted with adding value and keeping themselves and the employers accountable to agreed outcomes. The absence of trust from employers leads to erosion of trust and loyalty from workers. The work-from-home arrangements that emerged as a result of the COVID-19 pandemic created a panic environment for many employers. A Harvard Business Review article highlights the “negative spiral in which manager mistrust leads to micromanagement, which then leads to drops in worker motivation, further impairing productivity” and this spiral became deeper with COVID-19 pandemic [73]. A recent Microsoft report highlights that 85% of leaders say that the shift to hybrid work has made it challenging to have confidence that workers are being productive [74]. Whether it is tracking remote workers, or those operating in a large physical setting (i.e. warehouses, shops) or mobile workers (i.e. drivers, delivery workers), or those who are Quiet Quitting, use of surveillance and productivity tools breaks trust relationships in unreparable ways [75] and can backfire to result in less productivity [76, 77].

Impact on health and safety: The increased pace-of-work and productivity expectations which leave no room for rest, thinking or corrective action leads to more workplace accidents [78, 79]. The “electronic sweatshop” requires repetitive, fast-paced work demanding constant alertness and attention to detail [80]. More repetition also leads to more severe physical injuries. Research literature shows increased stress associated with workplace performance scoring technologies [81–83]. Loss of autonomy over work, stress, and ubiquitous observation increases risk of psychological harm and mental health problems for workers [67].

Sometimes employers frame the productivity scoring systems as ‘games’. In other words, under the guise of turning work into competitive metrics, employers pitch workers against each other. Employers make the productivity metrics visible to all, potentially causing further stress on the workers. Even when such competition is used as part of a wellness program, the normative judgements of fitness and health are imposed upon workers. For example, expecting workers to meet certain fitness standards, and then making the metrics of those not fitting the ‘expectations’ (i.e. weight loss trackers) visible to everyone can be considered a form of body-shaming. The race to meet the demanded metrics, stress and the toll on physical health eventually leads to worker burnout [84]. In workplaces where one worker is easily replaceable by another without consideration to the human behind the data, and in the absence of any legal consequence, employers do not have any incentive to improve conditions.

Feedback loops and behavioral change: Algorithmic decision-making systems change the behavior of users and those who are impacted by the outcomes of these systems. They change and shape the culture and priorities of the implementing organization in many ways. By incentivizing workers to focus on a particular task rather than innovation and experimenting, “the organization sends a message to its workers simply by the tasks it chooses to monitor [85].” Productivity systems may result in unintended consequences of workers spending more time doing a particular activity, which is counted and rewarded, than achieving results. The metric becomes an end in itself. Surveillance works to discipline workers to conform to expected behavior which can be measured [64]. When worker’s autonomy and agency are reduced, the result is also a reduction in the capacity to be creative and “the ability to think or sometimes act out of the box [35].”

When workers are under surveillance and worry about their scores impacting their compensation or the future of their work, they will also naturally shift into more self-protecting behavior. Instead of collaborating with their co-workers or sharing their knowledge about more efficient ways of completing tasks, individual workers might become more private, distrustful of others and competitive [86]. They might also feel the need to game the system. Whether this need emerges as a reaction to the oppressive actions by employers, or whether from a need to increase one’s scores and possibly wages and benefits, gaming the system means finding ways to make it look like one is being productive, but in reality refusing to do what is expected. As a response to lack of trust from the management, workers can seek to circumvent intrusive managerial oversight [87].

Hypervigilance about continuous surveillance and dataification also demoralizes workers and takes away from other tasks that may be meaningful or necessary for long-term
wellbeing. Scoring only certain kinds of activities can force the workers to make decisions quicker without having the time to delve deeper into an issue, case or condition. Some researchers even suggest, for example, gamified systems in the workplace could complicate and subvert ethical reasoning [88, 89]. For jobs which require more frequent decision-making, such as health, human or social services, such behavior change can result in catastrophic consequences for people dependent on decisions made.

Shoshana Zuboff highlights that at the workplace “invasive technologies are normalized among captive populations of employees [90].” When an individual accepts work surveillance and scoring technologies as inevitable, the result can be a normalization of similar technologies in other parts of life. The individual internalizes the scored society [91] and invasive and questionable techniques are normalized. Pasquale and Citron warn us that “the menace of scoring in the Big Data economy is the volume, velocity, and variety of information that could be fed into a score, and that these scores could become decisive [53]” in a variety of different contexts. Already a spectrum of products are in use to score an individual, ranging from when assessments for a credit, insurance, employment, education, immigration, or even criminal justice. The practices workers are forced to accept in workplaces will not stay limited to employment decisions.

### 4 The roadmap

There are several policies that can be deployed to better protect workers from growing digital surveillance and productivity scoring systems. Circling back to the existing policy and regulatory commitments of the US, we can establish a path forward.

#### 4.1 Extend 1974 privacy act protections to labor regulations

FIPs were inspired by the Code of Fair Labor Practices and the Fair Labor Standards Act (FLSA, establishing minimum wage, overtime pay, recordkeeping, and child labor standards for workers in both the private and public sector) [8]. FIPs “set out the rights and responsibilities for the collection and use of personal data...with emphasis on actual practices or standards, as well as legal rights [92].” When Congress concluded the Privacy Act of 1974, eight principles were included to govern information about individuals maintained in federal agencies databases. Going back to the original inspiration, labor regulations should be updated. The 1974 Privacy Act’s protections should be extended to existing labor laws. Responsibilities of employers and rights of workers must be clear.

- **Collection limitation/Data minimization:** employers must only create, collect, use, process, store, maintain, disseminate, or disclose data directly relevant and necessary to accomplish a legally authorized purpose.
- **Data quality:** data collected must be relevant to the purposes for which they are sought to be used by employers. Accuracy, relevance, timeliness, and completeness of the data must be ensured by employers.
- **Purpose specification:** employers must be transparent about their intended use of the data prior to collecting any data.
- **Use limitation:** when employers collect data for the disclosed purpose, they cannot deploy the data they collect outside of the originally intended purpose of collection.
- **Security safeguards:** employers must ensure the data they collect is safely stored.
- **Individual participation:** Workers must have the right to receive data which has been collected about them or confirm whether this data has been collected, have the data relating to them communicated reasonably soon, and have their data erased, rectified, completed or amended if they choose so.
- **Openness:** employers must be forthcoming about the ways in which they develop policies related to data collection.
- **Accountability:** employers must have an accounting mechanism ensuring the principles enumerated above are followed.

It is worth noting here that the European Union’s General Data Protection Regulation (GDPR) Article 5 lists all FIPs other than Individual Participation (which is covered in separate forms in other GDPR articles) [93].

When S. 516 Privacy for Consumers and Workers Act of 1991 was proposed, Marc Rotenberg and Gary Marx provided separate testimonies to the lawmakers [94]. Although the proposal did not pass at the time, it is worth noting their individual additions to strengthen any future labor legislation. Marx explained the techno-fallacies salient in worker surveillance practices, and offered:

- **Validity principle:** need to have reasonable grounds for having confidence in the accuracy and worth of the information collected;
- **Redress principle:** those subject to privacy invasions have adequate mechanisms for discovering and being compensated for violations; and
- **Safety net or equity principle:** a minimum threshold of privacy is available to all.

Rotenberg strongly supported the proposed legislation, requested backdoor exclusions to be removed, and added additional safeguards to include:
• **Worker participation:** Workers must be involved in shaping the technology impacting them. Employers wishing to collect data should seek for greater means of co-determination and ensure workers participate alongside employers in setting the terms according to which their data is used. In addition to individual participation of the worker, this could be a collective right for a group of workers to meaningfully participate in and co-decide in all matters related to how they are assessed. Such co-determination would include assessment of the impact of a possible algorithmic system, whether the system is a beneficial solution, and if yes, then decisions on relevant data, algorithm design and the governance of such systems.

• **Business responsibility:** the personal information collected on employees is safeguarded.

• **Human review principle:** technology should assist but not replace human judgment when important employment decisions are made.

### 4.2 Implementation of Blueprint for an AI bill of rights

The fact that employee surveillance systems should be designed with greater consideration of employee rights has also been emphasized in the recently released Blueprint. This document outlines a vision for the future development and use of AI systems, which respects rights, democratic values, and fundamental principles. The vision now needs implementation. The Blueprint especially recommends:

- “surveillance technologies be subject to heightened oversight that includes at least pre-deployment assessment of their potential harms and scope limits to protect privacy and civil liberties”, and

- “continuous surveillance and monitoring should not be used in… work…where the use of such surveillance technologies is likely to limit rights, opportunities, or access:”

The Blueprint reiterates fundamental rights, current civil rights and anti-discrimination legislation. Its underlying vision should be used as a tool to support existing employment laws, labor relations regulations, and workplace safety laws. The Department of Labor and the relevant federal agencies (such as the Equal Employment Opportunity Commission, National Labor Relations Board, and Occupational Safety and Health Administration) should include implementation of the Blueprint in their strategic plans. While existing legal framework and case law can remediate for harms, EEOC can also use some other tools in its toolkit, such as Commissioner Charge or directed investigation to identify possible systemic discrimination [40, 95, 96].

Noted earlier, workplace surveillance is much more common than it was before and it is therefore important and necessary that these agencies consider this issue as one that should fall within their remit.

### 4.3 More enforcement from Federal Trade Commission

In 2021, the Federal Trade Commission warned companies about unfair or deceptive practices, including the sale or use of biased algorithms. The warning succinctly highlighted companies should use “AI truthfully, fairly, and equitably”, or otherwise FTC would use its enforcement powers from FTC Act, Fair Credit Reporting Act and Equal Credit Opportunity Act. The agency recommended companies should (1) limit where or how they use AI models, in light of any shortcomings, (2) make sure that AI does not discriminate on the basis of race, gender, or other protected class, (3) embrace transparency and independent assessments, (4) not exaggerate what the product can do or whether it can deliver fair or unbiased results, and (5) be honest about the source of data used in the algorithms and how the outcomes will be used.

Commercially available worker surveillance and productivity scoring tools put both vendors and employers under the scope of possible FTC investigation. FTC’s warning allows companies to improve their practices and to hold themselves accountable first—“or be ready for the FTC to do it” for them [97].

### 4.4 Build better capacities across worker unions

Worker surveillance and productivity scoring tools can be used to oppress unionization in the first place, and then to weaken union protections. To effectively protect workers’ rights, unions need to build better internal capacity and capabilities.

- To echo workers’ rights scholar Dr Colclough, “unions need a foundation of knowledge on the different types of digital technology and importantly on the instructions given to artificial intelligence, algorithmic systems [98]” and “unions need to urgently revamp their strategies and find ways to cooperate across borders … and ensure that all workers, in all forms of work, have the same social and fundamental rights [99].” For those systems where both employers and workers find mutual benefit, the design and governance of the algorithms should include workers and their representatives [100].

- Unions should also use their knowledge as a tool to support both NLRB and FTC in their enforcement activities. Unions can provide information to NLRB on which employers are using surveillance technologies and therefore should be obliged to file Surveil-
lance Reports [52]. Unions can also inform FTC on which companies are not using “AI truthfully, fairly, and equitably”.

- Unions could also ask EEOC and The Office of Federal Contract Compliance Programs (part of the U.S. Department of Labor) to issue opinion letters tailored to questions on worker surveillance and productivity scoring algorithms. Such opinion letters could be used to clarify lawful practices and applications [40].

Algorithmic systems which violate fundamental human rights and human dignity should not be legitimized by principles [101] or through the use of risk management systems. They should not be used in the first place. The systems which can support the work conditions, work outcomes, safety and wellbeing of workers while benefiting the employers, on the other hand, should be designed, used and governed respecting the above safeguards.

Funding No funding was received by either author to assist with the preparation of this manuscript. One of the authors is an unpaid Editorial Board Member in Springer AI & Ethics journal.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References


Springer
66. Munger, C.: Tweet by @PoorCharlieBot. twitter.com/PoorCharlieBot/status/1529400245146333185 (2022)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
QUESTION
3. If you are a technology developer or vendor, please tell us about your experience developing or distributing automated worker surveillance and management systems, including
   a. The purposes for which employers adopt your products and how they deploy these products;

ANSWER
ActivTrak is a workforce analytics software as a service platform that analyzes digital work activity data for insights to improve how people work – in the office and remotely. It is not a worker surveillance tool.

ActivTrak helps organizations understand work habits and potential blockers to success, view organization wide productivity trends for agile decision making, and improve technology usage and workflows to optimize efficiencies. With ActivTrak, companies can share weekly work insights with managers and employees to guide progress and growth while safeguarding data privacy and the security of customers and employees.

It is possible to be up and running in minutes with ActivTrak — including platform configuration, agent deployment and organizational enablement — although many enterprises choose to manage their deployment over a 3- to 5-week period. The agent is deployed on company-issued devices to track data such as active applications, URLs visited and other digital activity.

ActivTrak has invested heavily in its data security practices, such as SOC 2 certification, and built industry-leading features that enable customers to gain the productivity insights they need while actively protecting the privacy of their employees. These features

Aggregate and anonymize data
Provide role-based and permission-based access control
Limit data collection to business hours
Give employees access to their data

The ActivTrak platform does NOT include intrusive surveillance features such as keystroke logging, camera access, video recording, email reading or counting.

Privacy protections are set by default to prevent capturing any sensitive data or PII (Personally Identifiable Information). These safeguards cover privacy needs across the full account, for users accessing data within our platform, and for licensed users with our software installed on their devices.

We also encourage customers to be transparent about data collection and collaborative about solving productivity challenges. Like most things, when employees are both aware and consulted on the solution, their buy-in is greater.

Companies today struggle to adequately address over-hiring, technology bloat, inadequate training and failed transformations. Our ability to embed ActivTrak data into the equation precisely where it's missing enhances customers’ ability to make decisions in ways they never have before, and to better navigate current economic challenges.

Our data allows these organizations to:

- Make data driven decisions about workforce policies and capacity planning
- Get instant visibility into how teams work
- Optimize productivity and boost performance
- Maximize resources and find hidden cost savings
- Put workforce data in context with other business intelligence
QUESTION
3. If you are a technology developer or vendor, please tell us about your experience developing or distributing automated worker surveillance and management systems, including

b. How the impact, performance, and efficacy of your products is audited and validated by you, employers, and workers;

COMMENT
ActivTrak's impact, performance and efficacy are audited and validated through a combination of internal testing and external audits from third-party firms.

ActivTrak uses a variety of metrics to measure the effectiveness of its software, including user adoption rates, productivity gains, improved employee behavior and increased focus time.

Additionally, ActivTrak has adopted the use of its own product and incorporated the data findings into its business practices. Company leaders and workers have a first-hand understanding of the data collection and impact of the solution. Data collected and reported on stems directly from the end user's computer and does not allow for any manual input or manipulation, maintaining the integrity of the data and allowing for ease of validation.

ActivTrak is consistently ranked as a top workforce analytics tools on leading software review sites including TrustRadius, Software Advice, Capterra and G2. The awards, many of which are based on customer feedback and reviews, are given to top software vendors across multiple categories whose products have exceptionally high ratings for customer satisfaction, usability and performance.

Please read this press release including the most recent accolades: https://www.activtrak.com/news/press-release-activtrak-earns-awards-from-leading-software-review-sites/
We have also established a wide base of customer references across a diverse swath of industries. Here is what just a few of them have to say

Manufacturing  Without ActivTrak’s employee productivity data for remote workers, we would have started pushing people to come back to the office. Instead, the data led us to expand our work-from-home program, and for the first time in our history, we’re actively hiring people from other states to work from home. — Head of Talent & HR

Banking: Our employees have become much more productive with their time. It also allows managers to see which of their employees are close to being overworked and which have the capacity to take a larger role. Overall, ActivTrak pushed our team to be more productive and provided the management team with insights into where they can provide more support   Manager, R&D

Insurance  ActivTrak has been a game changer in our business as it allows us to re adjust workloads, determine if an ‘overloaded’ employee was really overloaded, and allowed us to let employees work from home with the ability to know they are truly conducting business   General Manager

Retail  We found the impact analysis feature to be a fantastic addition to our ActivTrak reporting. Impact analysis allowed us to quickly see changes over time and across different departments letting us know that an intervention we made had a big difference on workforce analytics data and overall productivity This feature is a great addition to a terrific workforce analytics tool   — VP, People Operations

Real Estate: For newer employees who may be struggling but afraid to ask for help, ActivTrak is great at finding those people  We can see where time is spent on certain activities versus peers and offer guidance early on. — Director, IT

IT Software/Services: The biggest benefit we’ve seen is it’s really allowed our managers to take a look at the different business processes and tools we’ve provided our employees and have those conversations in terms of, are you spending time in the right type of tool, are you focused on what’s most beneficial to the company, or are there areas where we can improve? It really opened the line of communication, not only with the managers and the direct employees, but I would say even multiple levels up. — VP, Chief of Staff to the CEO

ActivTrak customers have also accrued impressive ROI, including

800K dollars in savings on unused software licenses
4.2M dollars in productivity gains by finding additional capacity equal to 60 FTEs
500K dollars in savings through billing reconciliation, a 4X ROI

To read more case studies, visit https://www.activtrak.com/customers/

Brandon Hall Group, a leading research and advisory firm, recently has this to say about ActivTrak

ActivTrak provides a real time view of workforce activities, giving an organization a dynamic view of goal achievement. ActivTrak is not just the guardian of productivity. It is also an invaluable tool for managing the well being of the employee  Naturally, you could be concerned about monitoring technology. ActivTrak has spent a considerable amount of time addressing employee privacy. The company has perfected its data anonymity process and created highly advanced privacy controls that alleviate this concern.
QUESTION
3. If you are a technology developer or vendor, please tell us about your experience developing or distributing automated worker surveillance and management systems, including:

- Whether you engage with employers to help them implement your products in ways that protect workers' rights, health, and safety—or otherwise take steps to help protect workers who will engage with your products;

ANSWER
Yes. ActivTrak is committed to providing solutions that enhance visibility and productivity using an ethical approach that is focused on transparency and collaboration.

During the implementation of the solution, ActivTrak will engage with employers to provide guidance on platform configuration that ensures employee privacy and safety.

Through the use of ActivTrak's Role-Based Access Controls, organizations can be certain that only those individuals that require visibility into employee data are granted access.

Please refer to the following link for more on ActivTrak's approach to employee privacy:
QUESTION
3. If you are a technology developer or vendor, please tell us about your experience developing or distributing automated worker surveillance and management systems, including

c  How you and the users of your products manage data collection, storage, and maintenance, including access to data by third parties;

COMMENT
ActivTrak Clients
Role-Based Access Controls allow account administrators to configure individuals' access to specific data and employee cohorts to meet the organization’s unique needs

Please refer to the following link for more information on ActivTrak's Role Based Access Controls

Additionally, admins have the ability to manage the data that is displayed through the use of Insight Privacy and Configuration features, including employee identifiers.

Please refer to the following link for more information on these features:

Data Collection
The ActivTrak Agent collects data by capturing website URLs and application title bar information. The agent does not use screen-scraping, camera access or keystroke logging. This collection method aids in avoiding collecting any type of PII, PHI or customer data.
Please refer to the following link for a full list of data points collected by the ActivTrak Agent: https://support.activtrak.com/hc/en-us/articles/360050977352 What Data Does ActivTrak Collect

Data Storage
ActivTrak has implemented measures to protect data from unauthorized access, ensuring that data is stored securely, and limiting access to data to authorized personnel only. ActivTrak has agreements in place with third-party service providers to ensure that data is managed under legal requirements and industry standards.

Please refer to the following link for detailed information on ActivTrak's approach to data privacy https://support.activtrak.com/hc/en-us/articles/4414165344795-Data-Privacy-Controls-within-the-ActivTrak Platform

Maintenance
ActivTrak strives to prevent the requirement of a planned maintenance window when all or part of the ActivTrak application is taken offline. In the event that ActivTrak requires the use of a planned maintenance window, notifications will be sent out at least 7 days prior to the scheduled maintenance which shall be scheduled to be performed outside of US business hours.

Third Party Data Access
For all service providers who may access ActivTrak production systems or who may impact the security of the ActivTrak production environment, written agreements shall be maintained that include the service provider's acknowledgment of their responsibilities for the confidentiality of company and customer data, and any commitments regarding the integrity, availability, and/or privacy controls that they manage in order to meet the standards and requirements that ActivTrak has established under ActivTrak’s information security program and as required by applicable law.

Please refer to the following links for more information
List of sub-processors: https://www.activtrak.com/activtrak-sub-processor-list/

Security & Compliance
The ActivTrak platform is Soc 2 Type 1 and Type 2 compliant, considered one of the highest standards for security accreditation. This validates that ActivTrak’s operational processes and controls meet the highest levels of security, privacy and governance.

Please visit the following link to learn more about ActivTrak’s certification https://support.activtrak.com/hc/en-us/articles/4410093680283
QUESTION
3. If you are a technology developer or vendor, please tell us about your experience developing or distributing automated worker surveillance and management systems, including

d  Whether you provide guidance to employers on your products and their appropriate use, including guidance on notifying workers about the use of technology, and offering opportunities for workers to consent to or opt out of data collection;

ANSWER
Yes. ActivTrak's onboarding and adoption program provides clients with guidance on the deployment of the solution, communication to its workforce aligned with the desired level of transparency, and configuration of the platform to ensure compliance with regulations that impose obligations on employers regarding employee data and employee's right to consent as well as opt out, such as CCPA (California Consumer Protection Act).

Please refer to the following link for more information on the configuration of ActivTrak for CCPA compliance https://support.activtrak.com/hc/en-us/articles/10220443941019 How to Configure ActivTrak-for-CCPA-Compliance
Please refer to the following link for more information on introducing ActivTrak to an organization https://support.activtrak.com/hc/en-us/articles/360041642772-How-to-Introduce-ActivTrak-to-your-Organization

In addition, ActivTrak has invested in self service enablement content which can be found in the ActivTrak Academy, and also built out a Productivity Lab, a dedicated team of subject matter experts with decades of experience and expertise in workforce productivity, information technology and data science, to help clients better leverage data to unlock productivity potential and business efficiency. The Productivity Lab recently published its annual State of the Workplace Report which provides the latest
workplace insights and trends around productivity, engagement and technology

To learn more about the ActivTrak Academy, visit https://www.activtrak.com/academy/
To learn more about the ActivTrak Productivity Lab, visit: https://www.activtrak.com/productivity-lab/
To download a copy of the 2023 State of the Workplace Report Productivity and Engagement Data Trends, visit:
https://www.activtrak.com/resources/reports/2023 state of the workplace research/
QUESTION
3. If you are a technology developer or vendor, please tell us about your experience developing or distributing automated worker surveillance and management systems, including any steps you have taken to ensure that the use of automated worker surveillance and management systems does not infringe on workers' rights.

ANSWER
ActivTrak has evolved from an employee monitoring tool to a privacy conscious, workforce analytics platform. This evolution began with the belief that productivity is not about surveillance or tracking, but rather about the insights that can be gathered from digital user activity in today’s modern workplace When analyzed, this data can provide insights into how work gets done, how teams interact, how employees can learn and improve in their jobs, and how results can be optimized These metrics benefit both employees looking for job enrichment and improvement, and employers looking for employee engagement and improved results

ActivTrak has taken the following steps to ensure that the use of its workforce analytics platform does not infringe on workers' rights:

- Intrusive forms of data collection via keystroke logging, camera access, video recording, email reading or counting are NOT supported
- Non-business activity details and sensitive data are EXCLUDED from reporting Screenshots, screen views, detailed title bars, URLs and subpages are NOT included
- Data history is LIMITED to 12 months, 6 months or 30 days based on tiered pricing, with the option to purchase additional data history add ons
- Customizable role-based and permission-based access control PROTECTS confidentiality User data can be anonymized and aggregated
Do Not Track list stops data collection of a user’s associated device
- Employees can have access to their own personal data and insights
- SOC 2 Type 1 & 2 certifications and end to end data encryption

By taking these steps, ActivTrak ensures that its workforce analytics platform is used in a responsible and ethical manner, respecting the privacy and rights of employees.
Hello I have been a rideshare driver for Uber and Lyft for approximately 7 years I am also a board certified behavior analyst.

I am commenting today to express some of my concerns regarding the algorithms both platforms use and how it could be potentially discriminating against drivers based on traits they cannot control (race, gender, disabilities etc.).

The issues with both apps are numerous. However there is one overarching issue that impacts almost all drivers whether they realize or not There is an enormous lack of transparency This lack of transparency is pervasive in both apps.

One example. Uber and Lyft are calculating fares for drivers based on unknown factors.

One example. Experiments have been conducted and demonstrate drivers (sitting right next to each other) are offered different amounts for the exact same trip Since Uber won’t reveal how and why their trips are priced the possibilities for why the drivers receive different offers remains unanswered. It could be based on age, gender, race, or any number of unknown factors

Another example is that both Uber and Lyft offer what call promotions to drivers These can entail extra money for completing a certain number of trips. It isn’t clear how and why these promotions are assigned to drivers As neither company reveals what the criteria to receive these promotions are it is possible it’s based on any factor including race, gender, disability status, or some other unknown factor. If both companies had clear objective criteria that a driver would to have meet to receive all gear promotions, we could rule out such factors.

Final example. Uber gives different information to different drivers based on known criteria. The his includes whether or not a rider is a “top tipper” The drivers that are informed a rider is a top tipper can
make a better decision in regards to the profitability of a ride. The factors that determine whether a driver receives these notifications are unknown.

Thank you for taking the time to read and consider this comment.
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information; Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0058
Comment on FR Doc # 2023-09353

Submitter Information

Name: Saiph Savage
Address:
Email: [redacted]
Phone: [redacted]

General Comment

I used to work for Microsoft as a Software Engineer and helped to create the surveillance technology of Clarity (https://clarity.microsoft.com/) I would like to bring to your attention some of the capabilities that these technologies have: They not only record people’s mouse and keyboard clicks, but they can also re-create videos of exactly what a person did on a particular website

Microsoft has these technologies installed in all of their websites and web products and so they have videos of how millions of end users are using their different technologies. Some of the things to consider:

- Tools like Clarity could be used by managers at Microsoft to stalk their workers and see what exactly they are doing at their jobs (e.g., how they use PowerPoint online, Online Microsoft Word, Github etc)
- Managers from outside Microsoft can install Clarity on their company web pages to stalk their employees and see in detail exactly what they are doing at their jobs
- End-users of a website are not informed that these technologies are on a particular website. This makes it easy for managers to stalk their employees without workers’ consent
- The workers who design these surveillance technologies can also be exposed to disturbing content and they may not receive any type of psychological support. For example, when I was working at Microsoft and created these technologies I was seeing videos of how people were searching for images on Microsoft Bing. I accidentally came across videos of people searching for photos of underage girls naked. The videos showed how people were searching for such content.

I think these technologies need to be better regulated so that an employer can not just install such
surveillance technologies on their websites to effectively watch over their workers. It is also important to think about the wellbeing of the workers involved in the creation of the surveillance technologies and the harms they may be exposed to.

I am attaching a screenshot of the Clarity interface that showcases the videos that people can see of how end users utilize a website. The videos can be used by managers to surveil their workers.

Attachments

Screen Shot 2023-06-03 at 7.21.00 AM
Discovery ads can also appear as recommended videos on a video watch page. But if you really want to focus on user intent, you can select just the search results, and this particular network setting is done at the campaign level. So if I'm looking at targeting just the YouTube search results, this is pretty much the only time that I would use keyword targeting for a YouTube campaign.

So now for my discovery ads, I will go add new keywords, I'm just going...
This is a tricky subject. There are certainly times when surveillance makes sense like police, but in the everyday workplace it just looks like one more layer of stress and control over workers. I would be very careful weighing into this area.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0060
Comment on FR Doc # 2023-09353

Submitter Information

Name: Jerome Maynard
Address: United States,

General Comment

Stop invasive surveillance!! It's just not right!
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0061
Comment on FR Doc # 2023-09353

Submitter Information

Name: Hugh Keleher
Address: United States,

General Comment

Automated surveillance in workplaces is an invasion of privacy!
General Comment

The rise of automated surveillance and management systems at workplaces has begun to affect the everyday lives of workers across industries, with restaurant workers being significantly impacted. This new technology, although promising in theory, can lead to intrusive monitoring, thereby infringing upon the rights and dignity of workers. Please stop this surveillance. Thank you.
Electronic surveillance of employees is intrusive and insulting. Employees are humans not automatons. Not to mention it mimics Oceania in the book 1984, which is certainly not something that is any way American.
GENERAL COMMENT

See attached file

ATTACHMENTS

UNITE HERE AI Comment OSTP 06142023
June 14, 2023

Mr. Alan Mislove
Assistant Director for Data and Democracy
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20504

Re: Request for Information: Automated Worker Surveillance and Management filed electronically and by electronic mail to workersurveillance@ostp.eop.gov.

UNITE HERE commends the Executive Office of the President’s Office of Science and Technology Policy (OSTP) for soliciting information on the prevalence and impact of automated worker surveillance and management.[1]

UNITE HERE is the largest hospitality workers union in the United States representing almost 300,000 hotel housekeepers, cooks, food servers, bartenders and others from Anchorage to Boston and Honolulu to Miami. During this era of new and evolving technologies, our members are more and more impacted by algorithmic management systems, surveillance and the general transfer of human relations to computer systems.

In 2018, UNITE HERE initiated a national technology program designed to get ahead of emerging innovations and prepare our members for the future. We have successfully negotiated new language in many of our contracts that requires employers to negotiate over the implementation and effects of new technology on workers. We do not oppose new technology out of hand; instead, our goal has been to ensure that technology makes jobs better and safer for workers and that our members are properly supported and not left behind.

As several hospitality companies have implemented new technologies, we have learned that the impact of so-called AI and Algorithmic Management on workers is a function of the human managers who utilize it.

We believe that AI/AM can be useful, but only if used as Algorithmic Guidance rather than Algorithmic Management. Algorithmic Management is a series of orders by a machine that a worker has to follow while algorithmic guidance makes suggestions that workers are free to override based on their knowledge of the situation, the workflow and knowledge of their own physical strengths and limitations.

In these comments, we want to focus on a technology that impacts hotel and casino housekeeping. By examining the particulars, we are able to draw some conclusions that can be applied more broadly.

It is important to understand the reality of the work performed by our members before discussing how technology impacts it. The job of a hotel housekeeper has the highest injury rate among hospitality workers. The largely female, people of color and immigrant workers push carts weighing several hundred
pounds over carpet, make up to 28 beds a day, scrub bathroom floors and perform other physically challenging work. Because of the intense physical nature of the work, anything that causes a speed up or that reduces the time available for a housekeeper to do her work creates a situation where, by hurrying, she could become injured. It is not unusual for long term housekeepers to experience chronic pain and injuries.

In pre-AI/AM technology times, a housekeeper was given a list of rooms to clean on a clipboard in the morning, and she cleaned them in the order dictated by her experience. In recent years, a variety of programs have been implemented that algorithmically manage the housekeeper. To be clear, these programs are sold by third-party vendors. These developers have failed to take into account the perspectives of end-users, the workers.

When given free reign, these programs “manage” a housekeeper’s day in ways that no human would. To understand the impact, we asked some housekeepers to keep a record of their daily work assignments. The program directed one housekeeper, in the course of cleaning 11 rooms (five on one floor and six on another), to alternate between the two floors four times and switch wings of the floor an additional three times.

This burdensome sequencing of rooms is a common complaint among housekeepers. The sequencing is not just annoying; it can have significant impacts on the health and wellbeing of the end user. When housekeepers have to spend time traveling between distant rooms, they are more likely to rush. Rushing can lead to injury.

Another hazardous situation involves the types of rooms that the program might assign. There is a difference between rooms where the guest checks out (a “check-out”) and a room where the guest remains for an additional night (a “stayover”). Stayovers rarely involve full linen changes or deep cleaning of the room. Check-outs, by contrast, do and are much more work and more physically taxing. Housekeepers who can choose the room cleaning sequence typically alternate between the two types. This gives housekeepers an opportunity to pace their work and helps minimize injuries by allowing them to reduce the strain on over-taxed muscles in between check-outs. However, when we asked housekeepers subject to the AI programs to record their room assignments, we found cases where all the check-outs were frontloaded on the housekeeper’s schedule.

These are not pre-ordained outcomes of the software. They are management decisions (or indecisions) about how to configure the algorithm that impact the health and wellbeing of the women who provide one of the most important services in the hospitality industry.

Algorithmic management programs are created by software designers and configured by managers, and reflect the biases and goals of the designers and the managers. The idea that such a program can substitute for the life experience and situational awareness of the human being doing the actual work is a harmful fallacy and is predicated on the idea that all workers are interchangeable cogs. We reject this notion. Every worker brings a unique skill set, experiences and capabilities to the job; experienced managers focus on getting the most out of each worker’s skills and supporting them in the things that are difficult. If the program is left to its own devices, this sort of algorithmic management bureaucratizes leadership—treating all workers the same rather than acknowledging their strengths and weaknesses.
We also want to recognize that these types of programs have increased job requirements for housekeepers. In the pre-AI/AM technology era, one did not have to be computer literate or even to have strong command of written English in order to master the job. The rise of housekeeping management programs has meant that housekeepers now need to have a fair degree of comfort with technology and (often) need to be able to communicate in written English. As you might imagine, this causes a fair bit of anxiety and stress for some workers.

With that in mind, we believe that there are several important traits that are necessary to ensure that the systems support human labor.

1. **Transparency**—the system needs to tell the human both the tasks for the shift AND the rationale behind any suggestions as to how or in what order those tasks should be accomplished.

2. **Guidance instead of mandate**—the end user (i.e., the worker) needs to be able to use her judgment to decide the how and sequencing of the work. Human situational knowledge will almost always result in better outcomes.

3. **Regular and ongoing training**—while developers usually advertise that their product is “intuitive,” in our experience, what is “intuitive” for a software designer rarely is for a front-line worker. To get the most out of the program and for workers to not feel additional anxiety and stress from the program, they need regular training, and trainings should take into account their lived experience as frontline workers.

4. **Negotiation**—at present, systems of AI/AM can be imposed on workers without their input. An important step for the future is making the implementation of new technologies more collaborative via negotiations between end users (i.e., frontline workers) and managers. We believe new technology implementation should be a mandatory subject of bargaining between unions and employers.

5. **Preservation of data, access to records and the ability to make corrections**—these systems often store massive amounts of data (essentially a worker’s entire work history on a minute-by-minute basis). First, we should not allow uncontrolled surveillance. Records should be kept only so long as they are needed and not indefinitely. Additionally, it is critical that workers or their chosen representatives have the ability to review the data that is preserved and correct, interpret or dispute anything that is taken out of context, fails to account for other inputs or contingencies, or represents a threat to worker or public safety and privacy concerns.

In closing, we want to reiterate a point that we made earlier: management needs to be done by human beings and workers need to be able to use their own judgment and override algorithmic management systems when necessary. AI/AM need to be tools that promote good management and work practices by increasing transparency, communication and workers’ control of their situations. AI/AM should not be allowed to manage on their own.

Within the hospitality industry, the systems are largely designed by third-party companies and they are designed to be sold to companies that are concerned about the bottom line. This means that the end user (the worker) experience of the program is only taken into account in so far as it helps to sell the product.

UNITE HERE, and its predecessor unions, has represented frontline workers in hospitality for over a century. We are now seeing the emergence of new technologies and AI-enabled tools that pose significant risks to the job quality, health and wellbeing of our members. Considerable work is being
done to invent new AI/AM technologies and bring them to market without seeking the input of the workers and their unions. This must change and the Biden Administration has an opportunity to impact how these innovations are implemented in hospitality and across the economy.

We have offered the perspective of frontline workers in hospitality who are experiencing AI/AM in their workplaces. I hope you will consider their views as you develop appropriate policy responses to these new workplace technologies.

Sincerely,

D. Taylor
International President, UNITE HERE
As a former Postal Service distribution clerk, the production surveillance only measured quantity. Service requires quality!
I'm opposed to pervasive workplace surveillance as a degrading attack on my personal liberties.
I oppose efforts and attempts to automate surveillance of people in this country when not necessary for on-site security. Such images and recordings can be used by governments for other reasons and should not be acceptable in a free society. We got along somehow without around the clock everywhere surveillance, and I suspect that a government trusted by its people can do so again. Further, a government supported and trusted by its people should have little need for such extreme measures as to keep track of our every movement, purchase or opinion.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0068
Comment on FR Doc # 2023-09353

Submitter Information

Name: Alex Stavis
Address: United States,

General Comment

NO to ANY/ALL AI.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0069
Comment on FR Doc # 2023-09353

Submitter Information

Name: Rita Meuer
Address: United States,

General Comment

Put yourself in their place? You would nit want it and it's not necessary.
You should not be spied on while at work.
We do not give up our privacy rights when we go to work. To expect otherwise is a stretch.
Intrusive surveillance invites sexual harassment and abuse especially by managers.
As a server, table-side tablets erode the meaningful customer interactions that make my job worthwhile. The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety. Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work. Surveillance software systems managing our shifts often disregard our personal needs. We need to feel valued, not just efficient. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
Surveillance is an invasion of privacy.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0075
Comment on FR Doc # 2023-09353

Submitter Information

Name: Leona McCann
Address: United States,

General Comment

Work is hard enough without being watched every second. I will not frequent an establishment that watches a person's every move.
Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding. This lack of humanity is going to be our downfall as functioning society. It reeks of totalitarianism.
Surveillance is anti-democratic, and a tool used by fascists and corporations to penalize marginalized people. End surveillance on citizens.
My clients report an increase in anxiety related to intrusive monitoring. I just can't see where this is a healthy trend.
Stop automated surveillance Now!
Stop the dehumanizing surveillance of employees.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0081
Comment on FR Doc # 2023-09353

Submitter Information

Name: James Deshotels
Address: United States,

General Comment

not a good idea.
workers have rights and must be protected. Workers are already under pressure to meet standards of employers and customers every day. they don't need to feel like everything they do is being watched all the time
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0083
Comment on FR Doc # 2023-09353

Submitter Information

Name: I Engle
Address: United States,

General Comment

Boycott All Companies who use spyware.
Surveillance is not for the workers, it is for the bosses.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0085
Comment on FR Doc # 2023-09353

Submitter Information

Name: Mary Casey
Address: United States,

General Comment

Enough.
Surveillance software systems managing our shifts often disregard our personal needs. We need to feel valued, not just efficient.
Workers were never asked if cameras were ok or not. Get rid of them in the workplace.
The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety.
Technology is a valuable tool when appropriate--this application is not appropriate. Ordinary, law-abiding citizens are being tracked like criminals in the name of 'productivity,' and it's not cool. We must reclaim our freedom from becoming a surveillance state now.
General Comment

Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work.
General Comment

The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety. Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work. Surveillance software systems managing our shifts often disregard our personal needs. We need to feel valued, not just efficient. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
General Comment

We need to put people first, not computers.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document:OSTP-TECH-2023-0004-DRAFT-0093
Comment on FR Doc # 2023-09353

Submitter Information

Name: Bill O'Brien
Address: United States,

General Comment

No workplace surveillance!
I believe that this technology is unsafe, and will only get worse as the technology evolves even more.
WHO IS WATCHING THESE PERVS
General Comment

The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety.
GET OFF THE ORWELLIAN TRAIN PLEASE!!!!!
This is invasive and disruptive. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding. It also interferes with being social with customers, which is important for business good will. Thank you.
Submitter Information

Email: [REDACTED]
Organization: SHRM

General Comment

Please See Attached for SHRM's Comment

Attachments

SHRM_OSTP_Automated_Worker_Surveillance_RFI_Response
June 14, 2023

By electronic submission: http://www.regulations.gov

Arati Prabhakar, Ph.D.
Director
White House Office of Science and Technology Policy (OSTP)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

RE: Request for Information; Automated Worker Surveillance and Management; (Document ID OSTP_FRDOC_0001-0004).

Dear Director Prabhakar:

SHRM is in the middle of marking its 75th year as the voice of all things work, workers and the workplace. SHRM is the foremost expert, convener and thought leader on issues impacting today’s evolving workplaces. With nearly 325,000 members in 165 countries, SHRM impacts the lives of more than 235 million workers and families globally.

SHRM recognizes the importance of safeguarding workers’ rights, opportunities, access, health and safety while ensuring that employers can make informed business decisions in the workplace. Employers leverage technology and management tools across many business functions, including measuring accountability, process improvement, performance feedback, workload management, attendance and adherence to company policy. With technological advances and increased computing power, organizations can now leverage data, rather than anecdotes or qualitative information, to evaluate the efficiency of HR processes, employee productivity, diversity and attrition.

Employers are increasingly concerned about issues related to the legal risk associated with remote work, violence in the workplace, identity and property theft, lowered productivity, and on-the-job accidents and injuries. Employers must find appropriate ways to minimize these risks, and the ever-increasing associated costs of litigation. As a result, many employers turn to new technologies to prevent injuries, misconduct and other types of loss. Employers must also be mindful of the differences in a patchwork of state laws. While guarding against these risks, companies also must balance their business interests with the reasonable expectations of the privacy of their employees.

The potential benefit of the use of any technology must be weighed against potential risks. SHRM has long been at the forefront of helping employers navigate their business, compliance and safety needs against other potential risks, including privacy risks. To this end, SHRM has developed a comprehensive toolkit and supplemental resources to assist organizations in managing workplace productivity, analysis and employee engagement.¹ The toolkit includes sample policies, information

on legal restrictions on workplace monitoring, workplace-based searches and navigating these issues for multinational organizations.

HR leaders and organizations are also increasingly looking to people analytics as a tool to address some of the most pressing workplace issues. People analytics can be defined as the practice of collecting and analyzing employee (or applicant) data to understand, improve and optimize business outcomes; and 72 percent of HR executives using people analytics say that this adds the most value to their company.2 SHRM’s new research report, The Use of People Analytics in Human Resources: Current State and Best Practices Moving Forward, offers insights into how artificial intelligence (AI)-driven people analytics are affecting work, workers and the workplace.

SHRM research found that 38 percent of HR professionals whose organizations use people analytics say that their organization is looking to start using or expanding its use of people analytics for employee productivity monitoring in the next five years. Additional SHRM data on people analytics collected in 2021 indicates that over half of U.S. workers are comfortable with their organization collecting their performance data (68 percent), demographic data (62 percent) and productivity data (58 percent).

Included in automated systems is AI, which plays an important role in the current and future of work. HR professionals are looking to AI technology and automated employment decision tools to meet the needs of their organizations, including talent acquisition, retention, performance management and much more. These innovations are being leveraged in the workplace to manage the full employee life cycle, from sourcing and recruitment to performance management and employee development. Today, 1 in 4 organizations report using AI to support HR-related activities3; and 43 percent of CHROs say they plan to invest more in AI/automation for HR activities.

While some of the technologies and applications mentioned in OSTP’s RFI may be new and unfamiliar to many, SHRM believes there is a strong conceptual foundation for balancing any competing interests between an employer’s business and compliance and safety needs against other potential risks, including privacy risks.

HR professionals are at the intersection of workplace innovation and the increasingly complex policy environment as policymakers begin to regulate and address evolving technology uses in the workplace. SHRM looks forward to partnering with the Biden administration as our members are well-positioned to lead the conversation on this developing issue to best address the current, and future, needs of the workplace.

Sincerely,

Emily M. Dickens, J.D.
Chief of Staff, Head of Public Affairs & Corporate Secretary

---

2 The Use of People Analytics in Human Resources: Current State and Best Practices Moving Forward.
3 SHRM 2022 Talent Trends Survey.
The rise of automated worker surveillance systems has turned workplaces into arenas of relentless scrutiny. Though proponents argue they increase efficiency, it’s clear that constant surveillance negatively impacts workers’ morale, dignity, and privacy rights. The Nazi's surveillance in workplaces (not concentration camps) and it didn't work. If you have no heart, please try to learn from their abysmal failures motivating productivity in the workplace.
Do not spy on workers who are just trying their best.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0102
Comment on FR Doc # 2023-09353

Submitter Information

Name: Lynette Bech
Address: United States,

General Comment

Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work.”
There are many people who are over 65 and work full-time. Put US under omnipresent surveillance and we'll bankrupt Social Security in a year. My employer doesn't need to know what I say when I'm driving the vehicle, nor what grooming/hygiene habits I (don't) have when on the road.
Wearable tech has no place in a restaurant environment: not front of house, not waitstaff, not bussing staff. Creating a culture where employees are trusted and valued through management philosophy and behaviors is essential; wearable tech monitoring is not.
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0105
Comment on FR Doc # 2023-09353

Submitter Information

Email: [REDACTED]
Organization: United Steelworkers (USW)

General Comment

See attached file(s)

Attachments

23 06 15 USW comments to WH OSTP re worker surveillance
June 15, 2023

Filed Electronically: regulations.gov
Docket ID: OSTP-TECH-2023-0004

RE: United Steelworkers comments on OSTP’s RFI on Automated Worker Surveillance and Management (OSTP-TECH-2023-0004).

To Whom It May Concern:

I write to you on behalf of the United Steelworkers Union (USW or Steelworkers). Our union is the largest industrial union in North America, representing 850,000 workers in steel, aluminum, and other metals; paper; rubber; glass; cement; mining; chemicals; refining; energy; utilities; healthcare; education; service; and other sectors. We appreciate the opportunity to provide comments to the Executive Office of the President’s Office of Science and Technology Policy (OSTP) on the prevalence and impact of automated worker surveillance and management.

Automated worker surveillance and the implementation of new technology is occurring in USW workplaces across industries. In many locations, USW members and their employers are learning together as the technology often does not function as intended or there are unanticipated capabilities. Technology has been implemented in many workplaces where the company has decided to continue to have humans duplicate the work of the technology. Our members cite lack of worker input, lack of communication or transparency from the employer, management turnover, inadequate training, and inadequate regulations as key problems with the adoption of technology in our workplaces.

USW local unions have a variety of experiences as far as the implementation of new technology goes. Ideally, when employers are implementing new technology, they would:

- Consult with local unions at the very early stages of considering new technology;
• Collectively bargain over the implementation of that technology, including recordkeeping and data retention, lookback timelines, whether data can be used for discipline, and other details;
• Conduct a full assessment of the health and safety hazards of new technologies with the union and implement appropriate training and hazard controls;
• Ensure that the implementation of the technology does not result in layoffs; and
• Commit to a plan to train and upskill the existing workforce to implement and maintain any agreed-upon technology using existing union employees rather than outside contractors.

The ideal conditions for implementation of technology do not always occur in USW-represented workplaces. Currently, collective bargaining is the most impactful way to prevent economic or physical harm to workers due to surveillance or other technology in the workplace. However, we urge this administration to advance public policy to prevent job loss, unreasonable discipline, and injury to workers from these types of technology. We also support policy to protect workers’ privacy and prevent employer surveillance of workers when they are “off-the-clock”.

Our members have cited numerous examples of automated systems to monitor, manage, and evaluate workers in USW-represented workplaces. Here are a few examples:

• In a USW-represented hospital, employee ID badges are on a tracking system that monitors when employees enter and exit patient rooms. The hospital management uses the badge trackers to monitor who is responding to call lights, when a call light is answered, when a nursing assistant enters a patient room, and how long they stay in the room. The employer will use data from the ID badge system to follow-up and confirm or refute an employee’s claims about where they were working at any given time.

• Multiple USW-represented healthcare facilities utilize medication dispensers to track when medication is pulled for a patient and which employee is pulling the medication. The medication dispenser data monitors the actions of workers for purposes of discipline when medications dispensed are delayed or inaccurate.

• At a USW-represented manufacturing facility, the company installed a set of cameras with artificial intelligence to review products at various stages as part
of the quality assurance process. If the cameras spot an irregularity, they stop
the production line so it can be inspected for compliance. To date, this has not
been used for discipline at this location when products do not meet quality
standards.

• An emergency medical services (EMS) company uses a system that
automatically dispatches the ambulances. The system “learns” response times
continuously by logging entry and exit times for workers at a hospital or a
geofenced area. The system routinely misjudges traffic, and predictions for call
times can be erroneous due to complicated medical situations once the EMS
technicians arrive on the scene. This creates a backlog of calls. Workers can
be disciplined for excessive call times.

• USW members who work for utility companies are routinely monitored by
systems installed in the trucks that they drive to customers’ locations or other
work sites. This technology monitors their location via GPS. It also watches the
workers as they drive and will record and/or send an alert if both hands are not
on the wheel and their eyes are not facing forward. This data is collected by the
multiple employers who use these types of technology. This data is often used
for discipline if calls take too long, if workers stop their trucks at a location other
than their call, and if the system records many instances of “distracted driving”.

Conclusion

Technology to monitor workers is becoming more common in USW-
represented workplaces. Collective bargaining between a union and the employer is
currently the most effective way to address workplace-specific implications of these
technologies and ensure that workers’ rights are protected. However, advancing
public policy could help. We urge the administration to ensure that workers are not
harmed in the implementation of new technology across industries.

Sincerely,

Anna Fendley
Director of Regulatory and State Policy

(b) (6)
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0106
Comment on FR Doc # 2023-09353

Submitter Information

Name: Judith Ackerman
Address: United States,

General Comment

Health and safety come first. we are all related to each other.
This kind of tech is intrusive and violates the rights of workers to operate in good faith with the trust of their employer.
General Comment

IT IS A VERY UNFAIR ADVANTAGE FOR COMPANIES WHO AGREE WITH THIS BEHAVIOR IT NEED TO BE ERADICATED IMMEDIATELY
Privacy is our right, stop endangering it. Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work. Surveillance software systems managing our shifts often disregard our personal needs. We need to feel valued, not just efficient. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
Surveillance of workers leaves room for lots of abuse.
The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0112
Comment on FR Doc # 2023-09353

Submitter Information

Name: Sherrill Futrell
Address: United States,

General Comment

Just another step in dehumanizing human beings - for money - by rich people who don't give a dam.
Saying that surveillance is to 'fight crime' is B.S.! Surveillance could all too easily be used for nefarious purposes, for tracking law-abiding citizens even when they are indulging in perfectly innocent activities. Somebody makes a wrong turn and just happens to be near 'suspicious' activity could be dragged in for interrogation. Privacy is precious!
Wearable tech for monitoring is intrusive. We need respect for personal boundaries at work.
It is extremely rare that a restaurant incorporates technology without compromising customer service. The absence of human connection between customers and kitchen staff will result in poorer products and less business. It alienates older and immigrant customers. It should only be used as a convenience and not imposed as a requirement. The incorporation of AI will ultimately result in some form of abuse and result in tremendous business liability.
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0116
Comment on FR Doc # 2023-09353

Submitter Information

Name: Sharon Paltin
Address: United States,

General Comment

Bad use of technology. Humanity is what is needed.
Workers should not be intruded on by surveillance. Workers need the space and time to do their jobs effectively without disturbance and interference from AI or spying tech.
Invasive surveillance invades people's privacy and makes them feel uncomfortable. That is why it should be stopped.
The rise of automated worker surveillance systems has turned workplaces into arenas of relentless scrutiny. Though proponents argue they increase efficiency, surveillance of workers is oppressive, disrespectful, and undignified. It negatively impacts workers’ morale and is an invasion of privacy.
The people who need to be watched via 24-hour surveillance are the bosses. They regularly engage in illegal activity, such as retaliating against workers who are trying to unionize, not paying required overtime, not allowing required breaks, lying on financial disclosure reports, etc. The surveillance also helps them find out who might have proof of their illegal activities and thus be able to sue them (not that the court system isn't already in their favor). Turn the cameras around and I won't have any complaint about them. But the direction they're facing now is the exact opposite direction of where in a just world they'd be facing.
The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety. Surveillance software systems managing our shifts often disregard our personal needs. We need to feel valued, not just efficient. Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work.
This sounds like a 'police state' but then we know that this country was established for the British elites. GREED
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0123
Comment on FR Doc # 2023-09353

Submitter Information

Name: Karl Moore
Address: United States,

General Comment

The
Stop treating workers like slaves
General Comment

Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding.
Wearable tech for monitoring feels intrusive. Restaurant workers need respect for personal boundaries on the job.
I am not a restaurant worker but I am an eater at restaurants. The provision of service in a restaurant, seating the dinners, providing menus, taking and delivering orders, checking on customer satisfaction, providing the bill, and accepting payment are all things that are accomplished, usually by waiters, and deserve decent, minimum wage (at least) payment. Waiters hustle in order to provide good service and earn their 'tips'. They do not need or deserve to be monitored by surveillance cameras. Neither do the customers.
Wearable tech for monitoring is intrusive. We need respect for personal boundaries at work.
General Comment

Enough is enough!
No workplace surveillance. A manager shouldn't so stupid as to not know what is going on. That's laziness. Someone got over-promoted,
I try to tip generously because servers and other restaurant personnel are doing all in their power to make a great experience for me. They deserve my support.
GENERAL COMMENT

Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding. On the business side of things, it will most likely hurt performance.
Too much surveillance in our country as is, don’t need it in restaurants.
This type of surveillance feels inhumane and I'm failing to see the benefit for workers. We need respect for personal boundaries at work and begin developing tools to actually improve our quality of life at work, not make it more challenging.
Kroger and Target use this to make sure shoppers don't leave the store without paying for their purchase, even at the Self-checkout lane.
Public Submission

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0138
Comment on FR Doc # 2023-09353

Submitter Information

Name: Ron Strochlic
Address: United States,

General Comment

Surveillance software systems managing shifts are intrusive and often disregard personal needs. Restaurant workers need to feel valued, not just efficient.
In these dire, uncertain times, working people do not need anymore stress.
The rise of automated worker surveillance systems has turned workplaces into arenas of relentless scrutiny. Though proponents argue they increase efficiency, it’s clear that constant surveillance negatively impacts workers’ morale, dignity, and privacy rights. It is very important to respect the rights and well-being of restaurant workers, and to say loud and clear: #StopTheSurveillance.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0141
Comment on FR Doc # 2023-09353

Submitter Information

Name: Mark Hayduke Grenard
Address: United States,

General Comment

Stop the constant surveillance at restaurants and workplaces.
I would never work at an establishment under the unblinking eye of cameras like the ones described in the email I received.
We need real people not high tech to treat customers with respect. It's not called 'Service Industry' for nothing!
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0144
Comment on FR Doc # 2023-09353

Submitter Information

Name: Brett O'Sullivan
Address: United States,

General Comment

Wearable tech for monitoring is appallingly intrusive. It is crucial to respect personal boundaries at work.
The AI restaurant layout manager disregards the human element – we need a balance that respects our health and safety. Wearable tech for monitoring feels intrusive. We need respect for personal boundaries at work. Surveillance software systems managing our shifts often disregard our personal needs. We need to feel valued, not just efficient.
Stop being big brother and stop corporations for spying on us all.
The AI restaurant layout manager disregards the human element – we need a balance that respects the health and safety of restaurant workers. Wearable tech for monitoring feels intrusive. Restaurant workers need respect for personal boundaries at work. Surveillance software systems managing the shifts of restaurant workers often disregard their personal needs. Restaurant workers need to feel valued, not just efficient. Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding for restaurant workers. Why not get feedback from customers instead?
Being evaluated by a computer system based on data metrics feels disheartening. It lacks empathy and understanding. It signals a MAJOR lack of trust and faith in the general daily Respectful and Caring actions of Restaurant workers. Make it less necessary and impactful!!
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0149
Comment on FR Doc # 2023-09353

Submitter Information

Name: John Sonin
Address: United States,

General Comment

Keep your eye's on your mission goal, not on 'taking' from others!
ARE YOU TRYING TO KILL US?!
Surveillance is too great an intrusion on one's privacy.
PUBLIC SUBMISSION

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0152
Comment on FR Doc # 2023-09353

Submitter Information

Name: Diane Olson Schmidt
Address: United States,

General Comment

I would not want any surveillance of any kind in any workplace period.
PUBLIC SUBMISSION

**Docket:** OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

**Comment On:** OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

**Document:** OSTP TECH 2023 0004 DRAFT 0153
Comment on FR Doc # 2023-09353

---

**Submitter Information**

**Email:** [REDACTED]
**Organization:** AvaSure LLC

---

**General Comment**

See attached file(s)

---

**Attachments**

RFI RESPONSE- AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT
AvaSure (the “Company”) provides the leading hospital virtual care platform to systems with nursing and staffing shortages that are challenged to significantly reduce labor costs without sacrificing patient health outcomes. Recently recognized by KLAS Research as the leader in reducing the cost of patient care, AvaSure is the pioneer in providing best-in-class, video-based AvaSure TeleSitter® and TeleNurse™ solutions. As a trusted partner of more than 1,000 hospitals, AvaSure combines remote patient monitors, virtual nurses and other providers on a single platform to enhance clinical care without placing any additional burdens on existing staff.

The Company’s platform is designed to ensure patients remain safe by allowing virtual patient observers to interact with patients to keep them safe when they are at risk of adverse events such as fall, elopement, tube dislodgment, self-harm, etc. TeleSitter Solution workflows using unlicensed, trained observers via streaming audiovisual communication allows nurses to provide direct care at the top of their license. In addition, TeleNurse Workflows, where more experienced nurses handle virtual discharges and are observing the patients and the nurses providing the care virtually, allows for improved patient care with better oversight, allowing improved care with fewer resources.

Software is designed to automatically track observer alertness so as to notify nurse managers if the observers are not properly watching or are not engaging with patients, as failure to do so will endanger patients. As this platform is a suite of patient safety tools, in addition to tracking patient safety, it is also keeping nurses safe because the observers prevent workplace violence against clinical staff from patients and other staff members.

Automated observer alertness was designed specifically as a health and safety feature as it keeps patients and nurses safe by ensuring observers are doing their job. The additional benefits are reduced cost in terms of liability and insurance and improved productivity. There are several other automated features that ensure the observer is properly operating the system in terms of alarm management and documenting adverse events. This ensures accurate reporting of events and responsiveness of care teams to emergent patient events.

Several of the automated features and data points developed within the virtual care platform have come at the suggestions of the clinical teams that are operating the platform and subject to observation and data collection.

De-Identified data gathered belongs to the Company and is licensed to each hospital system operating the virtual care platform. Hundreds of hospitals participate in the licensed data portal and use this data as a benchmark against all others in the system by certain categories of similarly situated hospitals for the benefit of quality improvement and improved patient care. The data is not otherwise commercialized save for internal research purposes.

The data and its use have an impact on improved utilization of the virtual care platform and management by the hospitals of their care teams. There are several instances of marked improvement in care by reduction in falls and other adverse events, improved scorecards and ratings from AHRQ, HCAHPS and Leapfrog. Further it supports improvement in meeting standards for accreditation of hospitals.

Data collection is not optional as it is a matter of patient safety or workplace safety in the units where deployed. Hospitals may reassign nursing staff to units where the virtual care platform is not in use in the
event they wish to opt out and do not wish to be subject to observation or automated observer alertness. However, nearly everywhere the virtual care platform has been deployed the clinical care teams have played a significant role in deciding to use and enculturate the platform and are supportive as it reverts the scope of their job back to why they became a nurse in the first place, by allowing them to spend their time at the bedside caring for patients and reduces administrative, non-skilled burden. Patient and caregiver satisfaction improves through the use of the virtual care platform.

It is important to note that the automated data gathering is designed toward continuous quality improvement for the end result of improved patient and caregiver safety and as such thousands of caregivers that are also members of organized labor unions appreciate the support they receive by the use of the virtual care platform to support them in doing their jobs. The best practice for development of these tools is for quality improvement and learning opportunities for improved workflow to make for a better care delivery system and ease the burden of the care teams providing the vital healthcare that is needed.

Some of the emergent trends within the virtual care platform industry are clearly linked to artificial intelligence and expansion of machine learning models. These are valuable tools that will allow for further automation and tracking of workers. The emphasis and guidelines should be focused on the best practice of quality improvement and learning opportunities. Systems used or designed to impugn workers for substandard performance metrics may well have a chilling effect on utilization of these tools for the greater good of improving quality of care by supporting worker/caregiver performance and easing their burden from an increasing task list of nonessential duties that fall outside of their professional skills.

We would recommend allowing the free marketplace and labor unions to find a happy medium to allow for fair automated worker surveillance and management and currently will defer to the Joint Commission with respect to any proposed regulatory recommendations that may lead to an impact on patient safety. Several sources for supporting information to this response are set forth below within the portal.

Continuous Video Monitoring: Readiness for Growth : Journal of Nursing Care Quality (lww.com)
Continuous Video Monitoring: Readiness for Growth - PubMed (nih.gov)
Impact of Patient-Engaged Video Surveillance on Nursing Work... : Journal of Nursing Care Quality (lww.com)
Ligature and/or Suicide Risk Reduction – Video Monitoring of Patients at High Risk for Suicide | Behavioral Health | National Patient Safety Goals NPSG | The Joint Commission
Dear Madam or Sir,

Further to the Notice by the Office of Science and Technology Policy about a Request for Information (RFI): Automated Worker Surveillance and Management, I would like to present hereby a contribution.

The attached files are:
- the contribution itself (23 pages)
- a preliminary report referred to in the contribution as item referenced under number 7 (16 pages)
- an annex to the contribution: an overview of legislation applicable in the United States against employment blacklisting compared with uses cases of discriminatory employment platforms described in the 2 above attachments (4 pages).

For any further information, please do not hesitate to get in touch.

Sincerely,

Alexandre Papajak

Attachments

Request for Information_Automated-surveillance
2021-08-04_Discrimination by default

Annex-to-RFI_blacklisting_uses-cases_platforms
<table>
<thead>
<tr>
<th>State and Statute</th>
<th>Employer actions prohibited (if intended to prevent a former employee from obtaining other employment)</th>
<th>Match with one or more use cases identified in the ecosystem of employment platforms?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alabama</strong></td>
<td>Maintaining a blacklist. Notifying others that an employee has been blacklisted. Using any other similar means to prevent a person from obtaining employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Ala. Code § § 13A-11-123</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Arizona</strong></td>
<td>The knowing exchange, solicitation, or gift of a blacklist. A blacklist is any understanding or agreement that communicates a name, or list of names, or descriptions between two or more employers, supervisors, or managers in order to prevent an employee from engaging in a useful occupation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Ariz. Rev. Stat. Ann. § § 23-1361 to 23-1362</td>
<td>A blacklist can be spoken, written, printed, or implied.</td>
<td>(here ; in written)</td>
</tr>
<tr>
<td><strong>Arkansas</strong></td>
<td>Writing, printing, publishing, or circulating false statements in order to get someone fired or prevent someone from obtaining employment.</td>
<td>Yes - eg. false or deliberately inaccurate statement on a) professional skills b) language skills - case seen on another platform : c) nationality / right to work permit which automatically prevents the targeted person to even be considered for work)</td>
</tr>
<tr>
<td>Ark. Code Ann. § 11-3-202</td>
<td>Publishing that someone is a member of a secret organization in order to prevent that person from securing employment.</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>California</strong></td>
<td>Preventing or attempting to prevent former employee from getting work through misrepresentation.</td>
<td>Yes, if false or deliberately inaccurate statement may be considered as misrepresentation, for instance a) professional skills b) language skills - case seen on another platform : c) nationality / right to work permit which automatically prevents the targeted person to even be considered for work)</td>
</tr>
<tr>
<td>Cal. Lab. Code § § 1050 to 1053</td>
<td>Knowingly permitting or failing to take reasonable steps to prevent blacklisting. In a statement about why an employee was discharged or left employment, implying something other than what is explicitly said, or providing information that was not requested.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td><strong>Colorado</strong></td>
<td>Publishing or maintaining a blacklist. Conspiring or contriving to prevent a discharged employee from securing other employment. Notifying another employer that a former employee has been blacklisted. Any employer that provides written information to a prospective employer about a current or former employee, shall, upon that employee's request, send a copy to the employee's last known address. The subject of such a reference may also obtain a copy by appearing at the employer or former employer's place of business during normal business hours.</td>
<td>Yes, as data is, by default, shared between all clients - employers or recruiters - accessing the platform</td>
</tr>
<tr>
<td>Colo. Rev. Stat. § § 8-2-110 to 8-2-114</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Connecticut</strong></td>
<td>Blacklisting, publishing, or causing to be published the name of any employee with the intent and for the purpose of preventing that person's engaging in or securing other employment. Conspiring or contriving to prevent an employee from procuring other employment.</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Florida</strong></td>
<td>Agreeing or conspiring with another person or persons in order to get someone fired or prevent someone from obtaining employment. Making threats, whether verbal, written, or in print, against the life, property, or business of another in order to get someone fired or prevent the procurement of work.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Hawaii</strong></td>
<td>Making, circulating, or causing the circulation of a blacklist.</td>
<td>Yes, applies to businesses owning, hosting or running these platforms, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>Hav. Rev. Stat. § 377-6(11)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Idaho</strong></td>
<td>Maintaining a blacklist.</td>
<td>Yes, applies to businesses owning, hosting or running these platforms in the United States</td>
</tr>
<tr>
<td>State and Statute</td>
<td>Employer actions prohibited (if intended to prevent a former employee from obtaining other employment)</td>
<td>Match with one or more uses cases identified in the ecosystem of employment platforms?</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Idaho Code § 44-201</td>
<td>Notifying another employer that a current or former employee has been blacklisted.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>Indiana</td>
<td>Using any means to prevent a discharged employee from obtaining employment. Upon written request, prospective employers shall provide job applicant with copies of any written communication from the applicant's current or former employers that may affect the possibility of employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Iowa</td>
<td>Preventing or trying to prevent, either verbally or in writing, a discharged employee from obtaining other employment. Authorizing or permitting blacklisting. Making false statements about an employee's honesty. If a company, partnership, or corporation authorizes or allows blacklisting of a former employee, it shall be liable for treble damages.</td>
<td>Yes</td>
</tr>
<tr>
<td>Kansas</td>
<td>Using words, signs, or any kind of writing to prevent or attempt to prevent a discharged employee from obtaining other employment. Any person, firm, or corporation found guilty of blacklisting shall be liable to the injured employee for treble damages and attorney's fees.</td>
<td>Yes</td>
</tr>
<tr>
<td>Maine</td>
<td>Maintaining or being party to a blacklist, either alone or in combination with others. Preventing or attempting to prevent an employee from entering, leaving, or remaining in employment by threats of injury, intimidation, or force. Preventing or attempting to prevent anyone from obtaining employment by means of a blacklist. Any person who violates this law can be found guilty regardless of whether he or she intended to cause the employee harm.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>Using intimidation or force to prevent or attempt to prevent someone from obtaining or continuing in employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Minnesota</td>
<td>Combining or conferring with another or other employers to interfere with or prevent a person from obtaining employment. Using threats, promises, blacklists, or any other means to get someone fired. Blacklisting any discharged employee. Verbally or in writing attempting to prevent a former employee from obtaining employment elsewhere.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>Montana</td>
<td>Refusing to respond to a former employee's demand for a written statement of the reasons for discharge while providing a statement of those reasons to any other person. Blacklisting by word or writing of any kind, or authorizing or allowing a company's agents to blacklist. Attempting, by written, verbal, or any other means, to prevent a discharged or former employee from obtaining employment elsewhere.</td>
<td>Yes</td>
</tr>
<tr>
<td>Nevada</td>
<td>For an employer or employer's representative: Blacklisting or causing any employee to be blacklisted; publishing any employee's name or causing it to be published with the intent to prevent that person from getting work. Conspiring or contriving in any manner to prevent discharged employee from procuring other work.</td>
<td>Yes</td>
</tr>
<tr>
<td>New Mexico</td>
<td>For an employer or employer's agent: Preventing or attempting to prevent a former employee from obtaining other employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>New York</td>
<td>Making, maintaining, distributing, or circulating a blacklist to prevent an employee from obtaining or continuing employment because employee exercised rights to organize, unionize, or bargain collectively. Informing any person of an individual's membership in a labor organization or exercise of protected labor rights in order to prevent them from obtaining or retaining employment.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>North Carolina</td>
<td>Preventing or attempting to prevent, by word or writing of any kind, a discharged employee from obtaining employment.</td>
<td>Yes (at least &quot;attempting to prevent&quot;)</td>
</tr>
<tr>
<td>State and Statute</td>
<td>Employer actions prohibited (if intended to prevent a former employee from obtaining other employment)</td>
<td>Match with one or more uses cases identified in the ecosystem of employment platforms?</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>North Dakota N.D. Cent. Code § 34-01-06</td>
<td>Maliciously interfering or in any way hindering a person from obtaining or continuing other employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Oklahoma Okla. Stat. Ann. tit. 40, § 172</td>
<td>Blacklisting or causing an employee to be blacklisted. Publishing or causing employee's name to be published with the intent to prevent the employee from getting work. Requiring employee to write a letter of resignation with the intent to prevent or hinder other employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Oregon Or. Rev. Stat. § 659.805</td>
<td>Blacklisting or causing any discharged employee to be blacklisted; publishing or causing the name of any discharged employee to be published with the intent to prevent the employee from getting or keeping work. Conspiring or scheming by correspondence, or by any other means, to prevent a discharged employee from obtaining employment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Rhode Island R.I. Gen. Laws § 28-7-13(2)</td>
<td>Making, maintaining, distributing, or circulating a blacklist to prevent an employee from obtaining or continuing in employment because employee exercised rights to organize, unionize, or bargain collectively. Informing any person of an individual's membership in a labor organization or exercise of protected labor rights in order to prevent them from obtaining or retaining employment.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>Texas Tex. Civ. Stat. Ann. Art. 5196(1) to (4) Tex. Lab. Code Ann. § 52.031</td>
<td>Blacklisting or causing to be blacklisted. Preventing or attempting to prevent by word, printing, sign, list, or other means, directly or indirectly, a former employee from obtaining other work. Communicating, directly or indirectly, information about an applicant without giving the applicant a copy of the communication, and the names and addresses of those to whom it was made, within ten days of demand. Receiving a request, notice, or communication preventing, or calculated to prevent, the employment of an applicant without giving a copy of the communication to the applicant, and the names and addresses of those to whom it was made, within ten days of demand.</td>
<td>Yes, applies to businesses owning, hosting or operating these platforms in the United States, and potentially as well as to their clients - employers &amp; recruiters</td>
</tr>
<tr>
<td>Utah Utah Code Ann. § 34-24-1 to 34-24-2 Utah Const. Art. 12, § 19; Art. 16, § 4</td>
<td>Blacklisting or causing any former employee to be blacklisted, or publishing or causing the name of any former employee to be published, with the intent or purpose of preventing the employee from obtaining or retaining similar employment. Exchanging blacklists with or among railroads, corporations, associations, or persons. Maliciously interfering with any person's obtaining or continuing in employment with another employer.</td>
<td>Yes</td>
</tr>
<tr>
<td>Virginia Va. Code Ann. § 40.1-27</td>
<td>Willfully and maliciously preventing or attempting to prevent, verbally or in writing, directly or indirectly, a former employee from obtaining other employment.</td>
<td>Depends on legal meaning of 'willfully &amp; maliciously')</td>
</tr>
<tr>
<td>Washington Wash. Rev. Code Ann. § 49.44.010</td>
<td>Willfully and maliciously sending, delivering, making, or causing to be made, any document, signed, unsigned, or signed with a fictitious name, mark, or other sign; publishing or causing to be published any statement, in order to prevent someone from obtaining employment in Washington or elsewhere. Willfully and maliciously blacklisting or causing a person to be blacklisted, by writing, printing, or publishing their name, or mark or sign representing their name, in a paper, pamphlet, circular, or book, along with a statement about that person for the purpose of preventing employment. Willfully and maliciously publishing or causing to be published that a person is a member of a secret organization in order to prevent them from obtaining employment. Willfully and maliciously making or issuing any statement or paper in order to influence or prejudice the mind of an employer against a person seeking employment, or to cause someone to be discharged.</td>
<td>(Depends on legal meaning of 'willfully &amp; maliciously')</td>
</tr>
<tr>
<td>Wisconsin Wis. Stat. Ann. § 134.02</td>
<td>Any two or more employers joining together to: • prevent any person seeking employment from obtaining employment • cause the discharge of an employee by threats, promises, circulating blacklists, or causing blacklists to be circulated • prevent or attempt to prevent, by blacklist or any other means, a former employee from obtaining other employment • authorize or allow any of their agents to blacklist a former employee. Giving any statement of the reasons for an employee's discharge with the intent to blacklist, hinder, or prevent the discharged employee from obtaining other work.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Digital employment in France and protection of personal data: towards "discrimination by default"?

Report published in French on July 13, 2021
English version: August 4, 2021
Independent research led by Alexandre Papajak

Purpose of the Report - Introduction

After setting the general context of this research, recalling the importance of work and the reality of organized discrimination, this report will present the first findings about practices in the field of digital employment in France, and how these practices affect the rights and freedoms of natural persons, eg. Data Protection and Fundamental Rights.

This report will therefore address the following questions:

• what are the "marketplaces" in relation to digital employment
• how do they differ from the classic cv-libraries, with which they should not be confused
• what are the most problematic use cases identified in these platforms
• what is the scope of the labor market involved in these practices
• what impact do these practices have on the rights of individuals and the qualification the presumed infringements may receive under the GDPR, in terms of fundamental rights and in other areas of law.
Table of Contents

I) General considerations on employment and organized discrimination.................................3
   A) The importance of work from a social and economic point of view.................................3
   B) Organized discrimination in the field of employment: a caricatured but very real fact.........................................................................................4
      1°) The blacklisting scandal in the UK construction sector (discovered in 2009)..........4
      2°) The monitoring system at H&M by management and HR (fined in 2020)........5

II) Digital employment in France and personal data protection: initial findings.........................6
   A) An opaque ecosystem, where even supposedly competing companies collaborate...6
      1°) Quick typology of sites related to digital employment........................................6
      2°) Distinction between classic cv-libraries and employment “marketplaces”........6
      3°) Scope of the employment market covered by these “marketplaces »..............7
   B) Focus on the most problematic identified use cases..................................................9
      1°) Candidate profiles can be created without the consent or even the knowledge of
          the interested persons..........................................................................................9
      2°) Evaluations / "vetting" of candidates not known to them but visible to all
          employers / recruiters accessing the platform....................................................9
      3°) Comments by employers/recruiters on candidates' profiles & resumes without
          their knowledge....................................................................................................10
      4°) Resources (consultants) market with price sharing between companies,
          including between so-called competing IT Services (ITS) companies.............11
      5°) Obstructing access to employment by providing false, (quasi) eliminatory or
          discriminatory information..................................................................................11
      6°) Explicit function of "disqualification" (aka « blacklisting ») of candidates not
          known to them but visible to all employers / recruiters accessing the platform.....12

III) Presumed infringements of several areas of law, including Fundamental Rights.............13
   A) Presumed breaches of personal data protection legislation (GDPR).........................13
   B) Presumed infringements of fundamental human rights.............................................14
   C) Presumed infringements of labor law and civil and/or criminal law.......................14
   D) Presumed infringements of competition law.........................................................15

Conclusions........................................................................................................................16
I) General considerations on employment and organized discrimination

A) The importance of work from a social and economic point of view

Professional activity occupies a very important place in the life of a great majority of people.

After a person’s last name and first name, profession or the professional field in which one works are very often among the first information that a person says about her- or himself when getting introduced to others; this information is also what is requested by public or private organizations in the context of many everyday activities.

Likewise, professional stability and income that work brings condition, for many of us and to a large extent, the universe of possibilities in other areas of life, such as social life or family life.

This primordial importance of work and the need for equality in access to it is thus recognized in the law, for instance in the French Constitution (1) as from its first article which stipulates:

"The law promotes equal access of women and men to electoral mandates and elective offices, as well as to professional and social responsibilities."

At the level of European law, the Charter of Fundamental Rights of the European Union (hereinafter, "the Charter") defines freedom to choose an occupation and the right to engage in work as a fundamental right (art. 15), just like the right to protection of personal data (art. 8), equality before the law (art. 20) or non-discrimination (art. 21).

Labor economics considers there is a labor market, where supply (employees, candidates, job seekers) and demand (employers) must be able to meet freely and without distortion, in order to guarantee fair competition, better salaries and ultimately, the public interest. In France, this market is monitored from an economic point of view by organizations such as the INSEE (3). Interestingly, the wording in social relations and employment inverts the economic common approach, speaking of “demandeurs d’emploi” (ie work demand) and “offres d’emploi” (employment supply).

On the other side of the Atlantic, one of the key messages articulated recently in a White House Executive Order to the Federal Trade Commission (FTC) was precisely about addressing, among other issues, the apparently widespread abusive practices of employers demanding to put non-compete clauses in employment contracts that systemically impede freedom of employment and also cause a lack of effective competition among some market participants on the business side (4). This issue was also considered by the US Department of Justice in 2019 and by the FTC in 2020 (4 bis).

In France, salaried employment is preponderant and represents more than 83% of total employment in the country (source: INSEE), to which is added more than 12% of various so-called independent statuses. Employment in the digital sector, which we will focus on,
represents more than 950,000 or 4% of employees in France (2017 figures from the SYNTEC, the French ICT Employers Union).

Thus, discrimination organized by economic actors against free access to work, whether for salaried employment or freelance contracts/assignments (whatever the legal status), not only undermines the fundamental rights and existence of the natural persons concerned, but also harms the general interest.

Sources:
(1) French Constitution of 4 October 1958
https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006071194

(2) Charter of Fundamental Rights of the European Union

(3) INSEE - labour market scoreboard - wages in France
INSEE : Institut National des Statistiques et des Etudes Economiques
https://www.insee.fr/fr/outil-interactif/5367857/tableau/50_MTS/51_EPA

(4) The White House - Remarks by President Biden At Signing of An Executive Order Promoting Competition in the American Economy (July 9, 2021)

(4 bis) US Federal Trade Commission - Non-Competes in the Workplace: Examining Antitrust and Consumer Protection Issues (quoting also action by the US Dep. of Justice)

B) Organized discrimination in the field of employment: a caricatured but very real fact

The fact that discrimination in employment can be organized, i.e. produced and maintained over a long period of time by a group of economic actors, is often caricatured or brushed aside, whereas it is a real fact. The main difficulty is to be able to bring to light these practices, which are concealed and denied by the very perpetrators of these acts, who rigorously follow a "law of silence".

We can remind here two reference cases about such practices:

1°) The blacklisting scandal in the UK construction sector (discovered in 2009)

In 2009, after eight years of investigation by an investigative journalist in contact with people who had been claiming to be "blacklisted" in their professional field for years, the Information Commissioner Office (ICO), the authority in charge of the protection of personal data in the United Kingdom, seized a database and a large number of documents held by a company managed by a single individual.
The latter was in contact with the largest construction companies in the country, and organized the disqualification of several thousand people, thus depriving them of employment for periods ranging from eight to twenty years. The companies that used this system had denied its existence for years, sometimes even defaming the victims who could think of this type of practice but could not prove it.

This scandal was the subject of a parliamentary report in the House of Commons (5), where MPs relayed the concerns expressed by employees and workers unions that these practices were likely to continue in 2014. The same MPs also noted, among other things, the lack of honesty on the part of the involved companies who, during collective negotiations to provide redress, made it appear through misleading wording that an agreement had been reached with the injured parties when this was not the case.

Source:
(5) British Parliamentary Report on the subject of occupational blacklists (House of Commons, Scottish Affairs Committee)

2°) The monitoring system at H&M by management and HR (fined in 2020)

On October 1, 2020, the Personal Data Protection Authority of the Hamburg Lander (Germany) reported a penalty of €35.3 million (circa USD 41.35 million) against the H&M retailer for their employee monitoring system (6) (7).

This system included organizing interviews between an employee and his/her manager each time an employee returned from sick leave. This was done in order to obtain as much information as possible about the reasons for the absence, including medical information such as symptoms. Everything was written down and stored, as were reports of seemingly informal conversations between managers and staff, which in reality were aimed at obtaining information ranging from unimportant topics to the employees' family difficulties or religious beliefs. This gathering of information could also be done digitally and made accessible to about fifty managers.

Here again, it was only through the intervention of the press, which relayed the content of a leak of personal data from this company, that the practice became known - apart from the directors, managers, and HR officers who were organizing it - and then sanctioned by the competent supervisory authority, which fulfilled its mission of protecting the rights of individuals.

Sources:

II) Digital employment in France and personal data protection: initial findings

A) An opaque ecosystem, where even supposedly competing companies collaborate

We will first make a quick typology of the websites related to digital employment (1°), before distinguishing the characteristics of the "marketplaces" from those of the cv-libraries, which should not be confused with them (2°), then describing the scope of the impacted employment market (3°).

1°) Quick typology of sites related to digital employment

Generally speaking, websites and platforms related to digital employment fall into five main categories (not exhaustive):

i Career pages of employers / contract jobs providers websites (large groups, IT Services, SMBs, startups, public employers, etc.);

ii Recruitment companies websites, serving employers from the above category (i);

iii Resume libraries (or cv-libraries), which are sites where candidates can apply to job postings published by employers (i) or recruiters (ii);

iv Job/assignment aggregators, which gather published offers that may come from websites in categories i to iii, and even sometimes iv;

v "Marketplace" platforms, which have various functionalities and can interact, in different ways, with sites belonging to the four previous categories as well as to the category v itself.

This first typology is not exhaustive, and does not intend to include all types of sites or platforms in SaaS mode related to employment, but it aims to remove the first level of opacity since it is easy to confuse these marketplaces with the four previous categories of websites whereas their functionalities and objectives are radically different.

2°) Distinction between classic cv-libraries and employment "marketplaces"

Once such a typology has been established, the main distinction to be made in order to measure the actual scope of the types of personal data processing carried out by the "marketplaces" consists in distinguishing them from classic cv-libraries.

In summary:

- In a cv-library, candidates put their resumes online to share them with employers or to apply for job offers. Employers and recruiters only have access to the information input by the candidates and shared by the latter with
the recruiters at the time of an application. It is therefore a one-to-one relationship between the candidate and the employer/recruiter;
- In the "marketplaces", employers and recruiters have various functionalities that allow them to collaborate with each other, give candidates ratings, comments, or judgments, etc. This totally distorts the relationship between candidates and employers or recruiters, since employers and recruiters now act as a "block" and share data with each other without the knowledge of the people they pertain to.

The table below lists the different functionalities observed to be available to employers or recruiters that are clients of these “marketplace” platforms, with an initial assessment of the risk of non-compliance with GDPR or other legal texts.

The sign (*) in the “Marketplace” column indicates that not all of the listed features are necessarily present on every site, but have been found on at least one of these platforms.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Cv-library</th>
<th>&quot;Marketplace&quot; *</th>
<th>GDPR compliance / other law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising of permanent positions or contracts</td>
<td>Yes</td>
<td>Yes</td>
<td>Green</td>
</tr>
<tr>
<td>Access to resumes uploaded by candidates</td>
<td>Yes</td>
<td>Yes</td>
<td>Green</td>
</tr>
<tr>
<td>Follow up of applications done by candidates</td>
<td>Yes</td>
<td>Yes</td>
<td>Green</td>
</tr>
<tr>
<td>Creating candidate profiles without their knowledge</td>
<td>/</td>
<td>Identified practice</td>
<td>Yellow</td>
</tr>
<tr>
<td>Assessment / &quot;vetting&quot; of candidates not known to them but visible by all employers / recruiters accessing the platform</td>
<td>/</td>
<td>Yes on some sites</td>
<td>Red</td>
</tr>
<tr>
<td>Comments made by employers / recruiters on candidates’ profiles &amp; resumes without their knowledge</td>
<td>/</td>
<td>Yes on some sites</td>
<td>Red</td>
</tr>
<tr>
<td>Market of resources (consultants) with sharing of prices (eg. Daily rates) between businesses, including between IT services companies supposedly competing with each other</td>
<td>/</td>
<td>Yes on some sites</td>
<td>Red</td>
</tr>
<tr>
<td>Hindrance to access employment with inaccurate or even false information that is discriminatory or (quasi) eliminatory</td>
<td>/</td>
<td>Identified practice</td>
<td>Red</td>
</tr>
<tr>
<td>Explicit &quot;disqualification&quot; feature against candidates, not known to them but visible by all employers / recruiters accessing the platform</td>
<td>/</td>
<td>Identified practice</td>
<td>Red</td>
</tr>
</tbody>
</table>

3°) Scope of the employment market covered by these "marketplaces »

The scope of the employment market covered by these sites includes indeed both salaried employment (with employment contracts) and employment in the form of assignments or contracting, regardless of the legal status (independent, freelance).
At the current stage of our research, about ten "marketplaces" have been identified and this type of sites is expanding, both in numbers (new marketplaces) and in size (each gaining more clients). For instance, some of these companies had a massive growth in 2020 in terms of capital, increase in revenues, additional offices, etc.

On these sites currently identified, it is possible to find mainly contracting job offers, but some of these platforms also advertise salaried job offers, in particular permanent contracts (in French “CDI”, *Contrat à Durée Indéterminée*, contract with undetermined duration).

Insofar, as our research has for the time being focused on the digital employment sector, the first observations are that:

- hundreds of ITS companies in this sector access this type of platform, directly or indirectly - eg.: one of these sites alone claims to have more than 300 ITS companies as clients, not mentioning clients in other business sectors;
- both permanent or contracting jobs are provided, to a large proportion, by these same ITS companies.

However, the actual scope of these sites covers many business sectors. Indeed, these platforms publish information about the customers they have, at least, in the following sectors:

- Telecoms
- Retail
- Startups
- Industry
- E-commerce
- Consumer goods
- Services
- Transportation

In addition, each of these studied platforms represents a significant part of the digital job market in France, either in terms of the number of candidates' resumes they keep, or in terms of the number of employers who are clients of the site, or in terms of the criticality of the punctual but discriminating service that they offer to employers (e.g. candidate evaluations / vetting).

In order to quantify these facts, the number of persons whose personal data are on these sites is between 4% and more than 40% of the total number of employees in the digital industry in France. That percentage is calculated according to the data provided by these websites and the total number of employees in the industry in France. However, as these platforms include offers for jobs based in other EU countries than France, these numbers suggest that it is very likely that these marketplaces are processing personal data of persons residing in other EU member countries too.

These elements show that the scope of the labor market affected by the practices of these platforms is significant, especially since some of these platforms are clients of each other or have common major clients (eg. groups/holdings with national and international presence), which increases the consequences of the practices of these marketplaces on the labor market.
B) Focus on the most problematic identified use cases

The following use cases detail the functionalities found in the different "marketplaces", in order to better highlight the problems they pose.

1°) Candidate profiles can be created without the consent or even the knowledge of the interested persons.

In the absence of valid consent given by the persons whose data are processed in this way, such action represents a first GDPR violation as no other legal basis allowing lawful processing of personal data under GDPR can be seriously invoked by those marketplaces.

However, this use case amounts before all to reducing people to the status of mere products or commodities, that can be added to a database and be the object of transactions or deals between buyers and sellers, without the concerned people even being informed about that.

This violation of the GDPR is clearly known to some of these platforms, as they engage in canvassing practices that appear to entice a natural person to create an account that, in reality, may have already been created but without their consent.

If this way of doing things is questionable in terms of ethics and compliance, the most critical aspect is of course the fact that this unauthorized creation by the marketplace owners of an account for a candidate is the *sine qua non* condition for being able to proceed with the other data processing or use cases, presented below, which infringe even more seriously the rights and freedoms of the persons thus put on records.

2°) Evaluations / "vetting" of candidates not known to them but visible to all employers / recruiters accessing the platform.

Once the profiles have been created, the candidates are evaluated or "vetted" on some of these sites.

While tests about technical matters, foreign languages, or other subject matters can be conducted in a transparent manner - with candidates having access to the results of these tests which can be later shared with recruiters or prospective employers - the criteria or wording of this evaluation or “vetting” is not shared or known to the people it concerns, which is obviously problematic.
Moreover, this evaluation or “vetting” is made accessible to all clients of
the platform, i.e. to a large number of employers and recruiters who see
this information when they discover the candidate's profile.

The typical risks of such massively distributed evaluation practices
(incomplete or inaccurate information, botched evaluation, evaluator
lacking the necessary skills to judge candidates, etc.) are multiplied by
the dissemination of such personal data and, important to remind it
again, without the knowledge of the persons concerned.

3°) Comments by employers/recruiters on candidates' profiles & resumes without their
knowledge.

This functionality is distinct from the evaluation or "vetting", carried out
by the organization in charge of the "marketplace", in that these
comments are made by the clients of these platforms, i.e. employers,
recruiters, or companies that give orders or are intermediaries for
contracting jobs.

Here, any recruiter or employer can annotate a candidate's profile in the
platform at will, again without this data being known to the persons
concerned.

In the screenshot from one of these sites, we can see for example that
these subjective comments are attached to people's profiles, just like
factual information such as a degree or experience.

The risk resulting from that type of functionality is also obvious, as it
allows any employer or recruiter to cause discrimination or another type
of nuisance to a candidate in front of all customers of a platform.

That appears to be another blatant violation of the very principles of the
GDPR, which requires lawfulness, fairness and transparency.

Despite some commentators pretending that these principles would be
« mere opinions », GDPR articles and recitals, as well as in case law,
provide substantial context, definitions and examples as to how that kind
of practice can be appreciated in real-world situations.
4°) Resources (consultants) market with price sharing between companies, including between so-called competing IT Services (ITS) companies

ITSs companies frequently communicate about their alleged difficulties of finding "talents" but speak a bit less about their level of collaboration in their core business.

It is indeed possible to find on this kind of platform workspaces where such ITSs companies provide each other with "resources" - read: employees, consultants - in order to meet the needs corresponding to bids or contracts these companies have won with some end clients.

In the following example, we see an extract of the information shared between these companies that define profiles and also communicate commercial information, such as the daily price (cost) of services.

<table>
<thead>
<tr>
<th>City</th>
<th>Position</th>
<th>Daily Price</th>
<th>Location Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris (75)</td>
<td>Développeur Node JS</td>
<td>520 €</td>
<td></td>
</tr>
<tr>
<td>Paris (75)</td>
<td>Expert sécurité</td>
<td>570 €</td>
<td></td>
</tr>
<tr>
<td>Paris (75)</td>
<td>Expert sécurité</td>
<td>570 €</td>
<td></td>
</tr>
<tr>
<td>Toulouse (31)</td>
<td>Consultant technico-fonctionnel</td>
<td>500 €</td>
<td></td>
</tr>
</tbody>
</table>

This practice raises questions, particularly with regard to competition law, and seems to suggest that competition between these ITSs companies is in fact limited to know who gets the margin with the end client.

5°) Obstructing access to employment by providing false, (quasi) eliminatory or discriminatory information

The previously mentioned items 1°) through 3°) already pose significant risks to the rights of individuals or are already discriminatory by themselves, but this use case is a different finding.

The platform can indeed “simply” display false information that significantly damages the candidate’s chances in an immediate way, and as long as the false information in kept on record.

For example, recruiters' or employers' websites may ask candidates for information about nationality or the right to work in the country where the job or assignment is located. However, it has been observed that a platform may display a false status relating to someone’s right to work (e.g. "the work permit ends on...") which will, in many cases, lead to the undue elimination of the candidate.

This use case is compounded by obstructions to the rights defined by the GDPR (access, rectification) - see Part III) A here after - and also constitutes discrimination.
6°) Explicit function of "disqualification" (aka « blacklisting ») of candidates not known to them but visible to all employers / recruiters accessing the platform.

As we pointed out in I) of this report, organized discrimination in employment is often caricatured and denied, even though these facts are very real, as documented by the decisions of regulators or parliamentarians.

Blacklisting practices are often dismissed as so-called "urban legends," at least in public.

Here we provide evidence of such a blacklisting practice, or "disqualification" of candidates, via a feature identified in one of these platforms.

This finding firstly reveals the intention of the owners of this platform to be able to discriminate against candidates on the entire market.

If the mention of "freelancing" points to the contracting jobs or freelancing, the effect of such a practice also impacts access to employment with an employment contract, with regards to the actual scope of the employment market covered by these platforms, as it has been already shown in the section II) A) 3°) (see pages 7 and 8).
III) Presumed infringements of several areas of law, including Fundamental Rights

These initial findings lead to the identification of multiple presumed infringements of rights and freedoms of natural persons in several fields of the law:

- in terms of protection of personal data (GDPR);
- in terms of fundamental human rights;
- in labor law and/or civil and criminal law;
- probably also in the field of competition law.

A) Presumed breaches of personal data protection legislation (GDPR)

In terms of protection of personal data, without pretending to be exhaustive here, these marketplaces display infringements:

- of the very principles of the GDPR: lawfulness, fairness, transparency (art. 5)
- of the rules applicable to the lawfulness of processing (art 6)
- of the conditions applicable to the consent of persons (art 7)
- potentially, about processing of special categories of data (art 9)
- of requirements for transparency and information to be provided when personal data are collected directly or indirectly from individuals (art 12, 13 and 14)
- of respect for the rights of individuals to their personal data in terms of access (art. 15), rectification (art 16 and 19)
- most likely, of international data transfers, with regards to the location of some of these companies' offices and/or the terms of their privacy policies. Given the complexity of such an analysis, we reserve our conclusions on this matter for now.

With regard to the right of access, it was possible to observe different levels of non-compliance:

- frequent dilatory actions (eg. waiting 30 days before first, obviously incomplete response);
- partial non-compliance (ie. information provided is obviously incomplete);
- total non-compliance, including after follow up message or letter;
- deliberate destruction of retained information (nb: it can also constitute a criminal offense to intentionally destroy data, especially in the case when such data would provide evidence of another offense).
B) Presumed infringements of fundamental human rights

In addition to the right in terms of protection of personal data, the practices of these "marketplaces" relating to digital employment, as identified and described in this report, also infringe the fundamental rights of individuals, as defined in the Charter (see section I)A), pages 3 and 4).

These facts show blatant infringements of:

- the fundamental right to professional freedom and the right to work (art. 15)
- the fundamental right to equality before the law (art. 20)
- the fundamental right to non-discrimination (art. 21)
- of several fundamental rights to solidarity (Title IV)
- the fundamental right to freedom of enterprise (art. 16)

With regard to Solidarity (Title IV) of the Charter, the discrimination organized by these companies undermines the very basis of access to the fundamental right to social security and social assistance for the people targeted by such discrimination, while the French state imposes on job seekers "an obligation to take positive action to seek employment".

In order not to be excluded from social assistance, people are in fact obliged to perform "positive and repeated" actions to find work, whereas this discrimination produces the conditions for a systematic and long-lasting deprivation of employment, the consequences of which are self-perpetuating, not to mention the clients of such platforms who may still ask candidates to explain "gaps" in their cv's or resumes.

Moreover, when such discrimination occurs over long periods of time, as in the case of the blacklisting scandal in the United Kingdom (see Part I) B) 1°), page 4), the consequences of such violations also clearly undermine respect for the fundamental right to professional and family life (art. 7, 9 and 33 of the Charter).

Source:
French Labour Code, article R5411-11 (in French)
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038032918/

C) Presumed infringements of labor law and civil and/or criminal law

The facts described in this report may constitute multiple infringements of labor law and other laws, but they certainly show repeated and ongoing acts that affect the working lives of the targeted individuals.

Such acts have been provided for by law, which qualifies them as harassment, and describes them in articles L1152-1 of the French Labor Code (Code du travail) with
respect to employees and, more generally, in article 222-33-2 of the Criminal Code (in French Code pénal).

Source:
French Criminal Code, Article 222-33-2 (in French)
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI0000029336939/

There are other provisions in labor, civil or criminal law that might be infringed by these practices but these won’t be detailed in the current report as the focus is on Data Protection & Fundamental Rights.

D) Presumed infringements of competition law

The practices described in sections II) A) 2°) & 3°) and II) B) 4°) also probably reveal a violation of competition law, since the findings show:

- companies that are supposed to be competitors but working together to fill contracts, not on a one-to-one basis but via "marketplaces" where all the players present participate, creating an apparently mass collaboration;

- these same companies sharing commercial information such as prices, which can contribute to anti-competitive price agreements, tacit or not;

- that, insofar as some of the freelancers have an entrepreneurial status, the various evaluations, "vetting" and even more the explicit "freelance disqualification" functionality, which the clients of the marketplaces can use and abuse on the whole market, constitute factual obstacles to the arrival of new entrants and to free competition on this market.

These findings once again appear to identify practices that are contrary to the law, in particular the competition law applicable in France, and most probably in other members of the European Union, with respect to illicit agreements between economic actors or cartels (whatever the exact or legal naming of it may be).

Source:
French Ministry of Economy and Finance (in French)
https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Entente
Conclusions

The realities of digital employment in France, with regard to the practices identified in the "marketplaces" studied in this research, appear to present multiple infringements of natural persons’ rights in terms of protection of personal data but also in terms of other fundamental rights, as defined in the Charter of Fundamental Rights of the European Union.

Moreover, the ecosystem of companies involved in these practices goes far beyond the digital or freelance industry, and thus impacts the employment rights of workers or unemployed people in multiple sectors through discriminatory practices and even systems designed to disqualify candidates on the entire market.

Such facts are serious and can correspond to acts sanctioned by the Labor Code, in civil and/or criminal law.

These practices also distort the very foundations of the labor market in France, and also distort the conditions of access to social assistance for people without jobs, both in terms of the legislation applicable in France and in terms of European law.

The practices in question, which tend to develop with the multiplication of these "marketplaces" relating to employment, may also constitute, in particular with regard to the digital services companies involved, anti-competitive practices similar to a cartel (exact term to be defined).

In any case, these initial findings from our research, which confirm generic elements already communicated in 2019 and 2020 on several occasions to the attention of the authority competent in terms of protection of personal data, reveal a drift in digital employment towards "discrimination by default."

Such findings are more than worrying and call for genuine protection of people's rights, starting with those defined in the GDPR which can be achieved, in case of inefficiency of this way, by the mobilization of fundamental rights.
A contribution for

THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)

Request for Information (RFI):
Automated Worker Surveillance and Management

Inputs for the RFI - EU-based ecosystem of discriminatory employment digital platforms reaching the United States: towards “discrimination by default”?

Overview

Further to the publication of the request for information (RFI) from the Office of Science and Technology about “Automated Worker Surveillance and Management“, the purpose of this contribution is to provide awaited inputs for the RFI and share insights on an emerging ecosystem of EU(France)-based employment-related digital platforms infringing on workers’ rights for a number of years and that has now landed in the jurisdiction of the United States, posing numerous risks to workers’ rights that fit precisely within the scope of this RFI.

After presenting an overview of that ecosystem (Part I°), this contribution will follow OSTP’s Data and research-related questions listed in RFI section 4 (Part II°) to share inputs, either pertaining to that ecosystem or to other automated systems related to worker surveillance.

This contribution will then raise some matters (Part III°) which are, in our opinion, related or could contribute to the subject of this RFI such as: recent NYC bill on automated employment decision tools (AEDT) - employment discrimination against the unemployed & long-term unemployment - bias in employment against financially underserved communities: the example of cyber jobs - US-UK data bridge & potential risk of abusive automated employment blacklisting via the CIFAS EIFD – DoJ recent no-poaching case in Connecticut and the concept of buyers’ cartel in competition law - the recent initiative from US lawmakers against data brokers. This will lead us to address the questions on policies, practices, or standards that could protect workers, as listed in RFI section 5 (Part IV°).

Notice:
As there is a policy to make the content of these contributions public, a certain level of information can not be provided at this stage, such as names of business directly or indirectly involved in the described practices. For the same reason, minimum inputs can be provided at this stage in response to RFI Section 1. about worker’s perspective while answers to this section would bring direct evidence to some of the questions asked in RFI Section 4. Data & research-related questions (and also bring SEC-related topics).
Preliminary considerations - references

This section lists the major regulations, guidelines or other documents considered while preparing this contribution for the OSTP:

1. United Nations - Universal Declaration of Human Rights (with focus, in this contribution, on workers’ rights)

2. Charter of the Fundamental Rights of the European Union (with focus, in this contribution, on workers’ rights)

   Nb : this recommendation is non binding but as it is used as a reference for data privacy as it inspired, at least in part, national or regional legislation.

4. Blueprint for an AI Bill of Rights

5. EEOC - FTC – CFBB joint statement about AI
   EEOC-CRT-FTC-CFPB-AI-Joint-Statement(final).pdf

6. US – EU terminology for AI

7. Digital Employment and Data protection in France : towards “discrimination by default”?
   Provided as attachment to this contribution.

8. TFUE article 101 and 102

9. OECD “Purchasing Power and Buyers’ Cartels – Note by the European Union”, 22 June 2022

10. Definitions of abusive practices according to the Portuguese Competition Authority

11. Definitions of collusive practices according to the Portuguese Competition Authority

12. Labour market agreements and competition policy by the Portuguese Competition Authority
    Best Practices In preventing Anti-competitive Agreements in Labor Markets

13. Proceedings from the European Commission against Amazon’s marketplace (France, Germany, Spain)

14. NYC bill on AEDT

15. Decision in no-poaching case from the DoJ brought to the District Court in Connecticut
I°) Overview of the ecosystem of discriminatory employment platforms

A°) Introducing the ecosystem

[1]. The ecosystem relies on a number of “dual mode” websites - on one side, a candidate/worker platform and on the other side, a business-to-business (B2B) platform - where features or uses cases have been recorded to infringe on workers’ rights by unfair or misleading data collection or sharing practices - not known to workers - up to the point of features causing them a high risk of discrimination, if not directly denying their “Right to work”, as defined in article 23 of the Universal Declaration of Human Rights [Ref. 1], or the professional freedom & right to work, as defined in the EU Charter of Fundamental Rights [Ref. 2]. These processing activities of personal data also appear to breach key privacy & data protection principles, such as those defined in the OECD since 1980 [Ref. 3] or other regulations.

[2]. Furthermore, at least some of these platforms provide features that may infringe on antitrust / competition law, for instance, by enabling horizontal collaboration among hundreds of IT service companies that are otherwise supposed to be competitors. Practices in that ecosystem may also be considered collusive or breaching other provisions of applicable competition law.

[3]. That ecosystem, nested in the 150+ billion euros French digital industry, has been impacting workers rights and creating barriers to entry to the IT service market in France for many years – for instance one of these platforms appears to have been set up back in 2013. However, since 2020, a growth acceleration has been recorded in their activity and at least two of the identified platforms are now based in or claim to be operating on the American market.

[4]. The practices enabled in that ecosystem pose serious risks to workers, including to their health and safety, equal employment opportunities, privacy, ability to meet critical needs and exercise of workplace rights ; these practices also appear to breach multiple laws at state level prohibiting employment blacklisting practices. As such, we also believe that these practices go also against the Administration’s commitment to ensuring that all workers have access to high-quality, well-paying jobs, including jobs with opportunities to organize and bargain collectively with their employers through labor unions, as articulated in the Executive Order 14025 (Worker Organizing and Empowerment) 6 and through a competitive market for their labor, as articulated in Executive Order 14036 (Promoting Competition in the American Economy).

B°) Facts and findings

[5]. The following paragraphs are based on the preliminary report titled “Digital employment in France and protection of personal data: towards "discrimination by default"?”, published in French on 13 July 2021, and translated in English on 4 August 2021 [Reference 7].
Quick typology of sites related to digital employment / recruitment

To start with a general and quick typology of sites related to digital employment / recruitment, dealing with publication of job adverts to collect applications from candidates, we can say that this type of websites and platforms fall into five main categories (not exhaustive):

(i) Career pages of employers / contract jobs providers websites (large groups, IT Services, SMBs, startups, public employers, etc.);

(ii) Recruitment companies websites, serving employers from the above category (i);

(iii) Resume libraries (or cv libraries), which are sites where candidates can apply to job postings published by employers (i) or recruiters (ii);

(iv) Job/assignment aggregators, which gather published offers that may come from websites in categories (i) to (iii), and even sometimes (iv);

v) “Marketplace” platforms, which have various features and can interact, in different ways, with sites belonging to the four previous categories as well as to the category (v) itself.

This first typology is not exhaustive, does not intend to include all types of sites or platforms in SaaS mode related to employment (eg. Application Tracking Systems, “ATS”, or s tools with a single specific purpose), but aims at removing a first level of opacity since it is easy to confuse these marketplaces with the four previous categories of websites whereas their features and objectives are radically different.

Main distinction between "marketplaces" and standard cv libraries/recruitment websites

Once such a typology has been established, the main distinction to be made in order to measure the actual scope of the types of personal data processing carried out by the "marketplaces" as well as their effects, consists in distinguishing them from classic cv libraries.

In summary:

- In a cv library or similar websites, candidates put their resumes online to share them with employers or to apply for job offers. Employers and recruiters only have access to the information input by the candidates and shared by the latter with the recruiters at the time of an application. CV can be found by employers or recruiters when candidates agreed to find them with a search. As far as job applications data is concerned, this is therefore a one-to-one relationship between the candidate and the employer/recruiter;

- In the "marketplaces", employers and recruiters have access to various functionalities that allow them to collaborate with each other, rate candidates or make comments on their resumes or profiles, etc. This totally distorts the relationship between candidates and employers or recruiters, since employers and recruiters now act as a "block" and share data with each other without the knowledge of the people these data pertain to.
Most problematic use cases identified within this ecosystem of marketplaces

The following problematic use cases have been identified in that ecosystem for now:

- Candidate profiles can be created without the consent or even the knowledge of the interested persons – they can be abstracted and managed as mere products;
- Evaluations / "vetting" of candidates not known to them but visible to all employers / recruiters accessing the platform;
- Comments by employers / recruiters on candidates' cv’s without their knowledge;
- A non-public market of resources (consultants), involving hundreds of IT Services companies supposed to be competitors sharing commercial information such as price and appearing to act as one undertaking – nb: one platform doing such business in the most obvious way appears to have recently refocused on the French market only.
- Obstructing access to employment by providing inaccurate or false, (quasi) eliminatory or discriminatory information;
- Explicit function of "disqualification" (aka « blacklisting ») of candidates not known to them but visible to employers / recruiters accessing the platform.

Breach of the principle of Openness (OECD) or Transparency (GDPR)

The openness principle from the OECD framework is defined as follows:

“There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."

The above listed use cases recorded on these marketplaces breach this principle, as a significant if not the main purpose of their usage is not made explicit to the workers or candidates.

Breach of the principle of Collection Limitation Principle (OECD)

The Collection Limitation principle from the OECD framework is defined as follows:

“There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

When such a platform creates profiles about data subjects without their knowledge or consent, that platform appears to be also breaching the principle of Collection Limitation principle.
[11]. Breach of the principle of Purpose Specification (OECD) or Purpose Limitation (GDPR)

The Purpose Specification principle from the OECD framework is defined as follows:

“The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”

This principle is for instance breached in this ecosystem when personal data from natural persons that are collected at the time of an application appear to be made available or at least known to third parties other than the company or recruiter these natural persons applied with.

[12]. Breach of the principle of Necessity (GDPR)

The uses cases listed in section [8] also breach the principle of necessity, as it can’t seriously argued that all the employers or recruiters dwelling on one of these platforms need or even would have a legitimate interest to know about such a broad set of data about an applicant.

[13]. Breach of the principle of Proportionality (GDPR)

The uses cases listed in section [8] also breach the principle of Proportionality, as for instance, allowing that comments made on a candidate’s profile or resume, linked to one specific application or job experience, be broadcast to hundreds or thousands of business client of such platform has disproportional consequences on the employments rights of these natural persons.

[14]. Use of automated systems to produce rankings of “best candidates” at marketplace level

These platforms also claim to provide to their clients – employers or recruiters – the “best candidates”, the “best talents”, etc. This means that these platforms are profiling candidates and/or producing an assessment. While such mechanisms existed for individual applications – and can result in discrimination -, what raises even bigger serious concerns is that such rankings appear to be produced at the marketplace level, which means that this ranking will impact candidates not for one specific position or application, but at the scale of that part of the employment market.

Moreover, in light of the serious risks of breaches of fundamental privacy / data protection principles already presented in sections [9] to [13], the fact that this ranking is produced without any transparency or even information as to how such ranking or selection is produced.

If questioned, a typical answer these platforms may put forward is that they “didn’t disadvantage anyone” but this doesn’t suffice: if they promote always the same profiles to be on the “top of the pile”, this type of processing is known, on other types of marketplace, to strongly influence the decision-making process, and result in a recurrent disadvantage to the candidates who, for whatever reason, wouldn’t be put on top of the list but at the back of it.
A further examination of these use cases and the associated risks of breaches or breaches already presented would be also very likely to show:

- a lack of assurance as to the principle of Data Quality (OECD) or Accuracy (GDPR);

- an extended risk of bias, “by default”, as broadcasting that nature of data about workers or candidates represents another significant factor of influence through the concept of bias, such as confirmation bias or anchoring bias among employers and recruiters on these marketplaces;

- increased risks for vulnerable candidates, such as those or coming from underserved communities who are less likely to get access to employment by knowing employers directly and therefore would have to submit their resumes and application via that kind of websites instead, with all that it involves in terms of additional risks of discrimination;

- a context reducing if not nullifying workers’ actual bargaining power while implementing, at the same time, a ground that favors employers’ and recruiters collusive practices in hiring, wages setting or other aspects;

- an opaque online space suitable for covert harassment of targets, such as former employees who resisted various types of abuse in the workplace or whistle blowers for the public interest, who could be retaliated against while the lack of transparency makes that targets can’t even suspect that such practices occur on websites deemed to be supposed to provide employment.

**Blacklisting / automated elimination of blacklisted applicants**

These platforms appear also to be enabling, directly or indirectly, features that result in “blacklisting” of consultants, workers or candidates.

*Nb : as a side note, we know that, for instance in technology, companies in the United States such as Red Hat are taking care to use inclusive terms and replace words such as “whitelisting” or “blacklisting” in the context of networking security by equivalent expressions such as “allow list” or “block list”. In the specific context of employment discrimination, this word is still kept as it is frequently the one used in US state laws to prohibit such practices.*

In the two platforms referred to earlier in this contribution, we have recorded that:

- in the first platform, a feature is providing a check box “freelance disqualified” (in French);

- the question of blacklisting was also asked to the second company, which declined to answer.

Across the United States, numerous local laws prohibit employment blacklisting in various ways and terms.

The legal information website nolo.com has been publishing, for more than five years, a list of laws prohibiting blacklisting in about thirty states.
This list of US laws applicable across the country can be found at the following URL: 

Based on this list of laws and the summary of their content, we have made a high-level review comparing these laws with the practices recorded in the platforms of that ecosystem that are now based in the United States or claim to be operating there.

The outcome of this review is attached as an annex to this contribution (4 pages) and tends to show that more than twenty states in the US may already laws in place that could tackle such blacklisting practices, including states with major economic activity such as:

- California ;
- Florida ;
- New-York ;
- Texas.

[18]. As a side note, there is also a law prohibiting blacklisting in Connecticut, where a very recent case brought to court by the Department of Justice (DoJ) has been judged in matters related to non-poach agreements. This will be further discussed in part III°) of this contribution.

[19]. In conclusion to this section, the research undertaken on this ecosystem that has been operating in France and in the EU for years, and that has landed recently in the United States:

- violate candidates’ rights to privacy and data protection, both in the EU and in the United States ;
- impact workers’ rights to be fairly considered for work, enabling marketplace-wide bias or discrimination and even engaging in illegal blacklisting practices ;
- provides a setting compatible if not required to engage in labor fixing, wages reduction to the prejudice of all citizens impacted by the outreach of these platforms, in the EU and in the US alike ;
- creates opaque conditions not required for fair access to work, increasing risks for the more vulnerable candidates, including from underserved communities, and may even serve as a place for covert harassment or retaliation against former employees or candidates, including against whistle-blowers.

[20]. As those two platforms are positioned at different levels, addressing different markets although with an overlap (the first one focuses more on large corporate end-clients, such as financial services or banks ; the second one addresses various industries, but seems to be more focused on start-ups), further research could be useful to further detail the extent of their anti-competitive practices that are providing an unfair advantage to their cartel(like) members against new entrants, businesses respecting fair competition but, before all, on the labor market.
II°) Data and research-related questions asked by the OSTP

a. What data and evidence exist on the prevalence of automated worker surveillance and management systems across different industries, occupations, and regions, including changes over time?

Firstly, we would like to detail or restate – just in case – why we consider that the discriminatory employment platforms are one kind of automated worker surveillance and management systems, and most probably a significant one.

This is because these systems, embedding various kinds of automated processing of personal data, are:

a°) the places where workers and candidates will more and more have to go to find and apply for work: their growth is accelerating, and what could be a niche a few years ago becomes an industry on its own;

b°) websites that are, in general, consumers of multiple online services – often vaguely referred to in privacy notices - that are themselves often based on automated systems. These online services would typically include resume/cv or degree online verification, credit check, or other forms of evaluations, more or less valid or automated, but still that can be shared online or used as inputs to produce the marketplace rankings of candidates, as presented in the section [14] here above.

As such, this type of platforms act both as the gate keepers of access to work, and as a place of choice to act as an aggregator of outputs produced by other automated worker surveillance and management systems. This feeds into question “i” herefater.

Then, as far as the ecosystem described in I°) is concerned, these platforms have a focus on digital employment but that kind of practices has spread to websites advertising jobs for any type of occupation, industry or region.

These websites share publicly the names of some of their largest clients, and these companies operate in the following industries (as listed in the attached report on discrimination by default):
- Telecoms
- E-commerce
- Retail
- Consumer goods
- Start-ups
- Services
- Industry
- Transportation

The above facts are documented and further evidence can be shared upon request.

Please note that, while evidence can’t be provided for the industry of temporary work, similar practices would take place in there as well.

While raising awareness on these platforms with a workers’ union representative back in June 2020, this person told me that he heard similar practices would exist in the temporary work
industry, but he added he never managed to get evidence of it, as these practices are covered by a climate of secrecy among managers and hiring staff. But the effects on workers’ rights that I have been told about were similar to the ones resulting from the practices are now documented.

Back to the two platforms present or claiming to operate on the US market, these are focused on so-called “freelance” workforce, which may, depending on the type of assignment, its relation to hierarchy in the commissioning organization or local regulations correspond to genuine provision of services or mere substitution of salaried workforce.

b. What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers’ pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

The practices identified and described in part I°) strongly suggest:

- that such automated workers surveillance and management systems introduce “discrimination by default”. As a consequence, they impact workers’ rights in many ways, starting with chances to get employed but also get a fair wage [see section 15.];

- that on one hand, candidates who get on “the top of the pile” [see section 14.] will get jobs, while those discriminated will incur incremental, self-repeating degradation of their professional prospects, directly impact their incomes, pay, benefits and health.

This impact on workers’ rights will be all the more severe that most workers are not informed of - or even don’t believe in – practices that go as far as blacklisting, many targeted workers or candidates who be be likely, in turn, to feel personally affected by these repeated rejections without understanding them. Needless to say that the less favored communities are, here again, likely to be the most impacted with regards to unequal access to other ways to work or relief.

Research data to get an objective and factual understanding of these impacts might be gathered with the help of various federal administrations such as the tax administration – as far as personal data may be used in the United States, once anonymized, for a research of public interest. Such data could be then used to define groups (clusters) of businesses, platforms or recruitment companies with different level of adoption of automated surveillance technologies and then, observe incomes, career evolution etc. of their employees, considering various factors (see question “d”). This could be joint initiative between OSTP and EEOC, FTC and/or CFPB.

c. What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers’ abilities to form and join unions and bargain collectively with their employers?

In our understanding, these platforms are the exact opposite of workers’ rights, as they represent a space that strongly favors employers’ if not organizes buyers’ cartels or even a monopsony.
Centralized databases enabling, directly or indirectly, employers or entities representing businesses’ interests to discriminate against or even to blacklist have been used to target members of workers’ unions or any worker raising concerns about health & safety, or any other valid concern. This was the case in the construction blacklist identified in the UK in 2009, which mingled such illicit blacklisting records with rather rare cases which should be dealt with by law enforcement, and not by a private database.

This construction blacklist destroyed thousands of live over periods of time going from eight to twenty years, destroying families, communities and causing even deaths. This scandal is described in the report on discrimination by default [Ref 7, page 4 & 5]. Although these facts go back to 2009, further alerts from workers’ groups or union in 2014 or later spoke of new occurrences of similar blacklisting practices. As part of this contribution, we will also mention the case of the CIFAS EIFD, a UK-based database allegedly design against organized, internal fraud in companies but which seems to whitewash blacklisting practices. In light of the new US-UK data bridge that has been agreed, this kind of automated system may get soon a footprint in automated workers’ surveillance and management in the United States [see III°].

Another sign that documents that these discriminatory employment platforms undermine workers’ right and are contrary to the rights of workers to organize is what happened when brought these practices to the knowledge of the French Data protection authority, in 2019 then in 2020, to several decision-makers in that authority. No action was taken to investigate these practices, or even to properly acknowledge the whistle blowing done about this matter of public interest. However, after we contacted some workers’ unions in France in September 2020, one of them responded offering their support on this matter but soon after, communications were cut. We realized one month later that the French DPA didn’t investigate the discriminatory platforms but chose to control workers’ unions instead.

https://www.cnil.fr/fr/fichiers-dadherents-un-syndicat-quelles-sont-les-bonnes-pratiques

This type of targeted control compared with deliberate laissez-faire in favor of automated surveillance & management systems appears as a clear hindrance of labor rights, and also echos the hostile climate towards social, racial and workers’ rights in the country, as recently raised by the United States and some other European countries before the United Nations.


d. What data and evidence exist on how the impact of automated worker surveillance and management systems differs across groups of workers, including based on characteristics such as race, national origin, sex, age, disability, religion, or health status?

We believe this question could be addressed in the same way and as part of the research approach identified in question “b” here above. The factors mentioned to in “b” implicitly referred to characteristics such as race, national origin, sex, age or also addresses or areas, which may indicate or be linked with social or economic uniformity. For characteristics such as disability, religion, or health status, we are unsure how it is possible to access anonymized, aggregated data but the principal to produce evidence would be similar as for question “b”.
e. What data or evidence exists on whether automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination?

We believe that our research about this ecosystem of employment platforms shows that these instances of automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination.

This can be further researched, in this ecosystem and in other types of automated worker surveillance and management systems.

To take one example, it should be feasible to check if Application Tracking Systems (ATS) or some of them, produce outputs that show discrimination.

Considering one protected characteristic - for instance, race or national origin – it could be possibly easy enough to identify relative differences between ATS as to the number of applicants with these characteristics and the number of selected candidates for interview, and those actually landing jobs.

As data needed to find out about these results could be anonymized and aggregated, it might be possible to access such data for a research in the general interest.

f. What data and evidence exist on whether automated workers surveillance and management systems impact employers’ ability to recruit and retain workers?

That’s a very interesting question, and while this contribution is focused on workers’ rights, we also believe that many employers may not be aware or realize what results get actually produced by automated systems, which are often working in a fairly autonomous manner.

Promises made by vendors of automated workers surveillance and management systems may not live up to the results of real tests, when such tests are carried out in an inquisitive way, such the MIT did for AI interview tools.

https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/

Employers may be misled by automated tools, especially when results of such tools are presented by vendors as scientific while they may actually be the output of simple, if not simplistic computations based on a few or even one Python function, for instance to compute the distance between two vectors made of word to declare a “match”. Such computation, as many others, may produce both false positives and false negatives.

As a result of the above, we believe that focused scrutiny of Federal agencies on at least some high risk or dubious types of automated workers surveillance and management systems could give incentive to vendors to deliver systems that bring genuine value to employers, while respecting workers’ right and minimizing risks of discrimination.
g. What data or evidence exists on how the provision of reasonable accommodations is accounted for in the design and operation of automated worker surveillance and management systems?

We don’t know that matter enough to provide specific inputs, but we believe that an approach combining elements outlined in questions “b”, “e” and “f” could be applicable.

h. What data and evidence exist on why employers decide to adopt automated worker surveillance and management systems?

We are unaware of such data today, but from various articles of press, employers decisions to adopt such systems may stem from:

- willingness for better efficacy or efficiency;
- concern to lag behind competition if not using the same tools;
- concerns about unethical or illegitimate actions from employees;
- efforts to reach more objective decisions, or to reduce bias by using more scientific approaches.

Such drivers could be further investigated by a direct survey with employers, or research on vendors website. Analyst firm, such a Gartner or Forrester could also provide valuable inputs.

i. Are there any existing or new systems that aggregate worker surveillance data across multiple employers?

The aggregation of those data is especially concerning, and this is precisely one of the concerns that we have because of the ecosystem of discriminatory platforms presented in part I°) of this contribution.

We are afraid though that this practice – to share applicants’ and application data even with companies or recruiters who were not the intended recipients of those applications – is not an isolated fact, as one ATS based in the United States brings forward the fact that they don’t engage in such practice as a proof of an ethical way to manage applicants’ data.

j. What are new or emergent automated worker surveillance and management systems—or new and emergent uses of existing technologies—that Federal agencies should be tracking?

In our opinion, Federal agencies could be tracking automated systems in a number of use case, or markets or circumstances. These could be defined upon strategic considerations and priorities adopted by each of these agencies or in joint initiatives – such as the joint initiative from the EEOC, FTC and CFWB on AI.
Just to name a few of those use cases, this tracking could deal with systems claiming to do:
- CV/resume or qualification verification and the sharing thereof;
- checks and/or management of so-called anti-fraud or internal fraud databases, other than official sources and including databases located abroad;
- assess undefined traits, such as “cultural fit” of candidates or workers, which may typically increase risks of discrimination or bias;
- any of the kind of AI processing activities confirmed as “high-risk” in the AI Act text that was just presented in the EU parliament.

An input that would be very useful for this question would be to start from an inventory of the main categories of automated worker surveillance and management systems – please see next question “k”.

**k. Where might further research, including by the Federal government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?**

Further research might be helpful in understanding the prevalence and impact of automated worker surveillance and management systems such as:
- getting an overall picture or an inventory of the main categories of automated worker surveillance and management systems;
- split each category into classes to get a finer understanding of prevalence and/or impact;
- identify the drivers – see question “h”;
- further analysis to get objective data on actual levels of systems maturity or efficacy;
- observe changes and evolution over time.

This might be seen as high-level road map, that can be of course further detailed.
A°) NYC bill on Automated employment decision tools (AEDT)

A new bill issued by the NYC Department of Consumer and Worker Protection (DCWP) regarding Automated employment decision tools is effective since January 1, 2023.

On DCWP official website, this bill is summarized as follows:

This bill would require that a bias audit be conducted on an automated employment decision tool prior to the use of said tool. The bill would also require that candidates or employees that reside in the city be notified about the use of such tools in the assessment or evaluation for hire or promotion, as well as, be notified about the job qualifications and characteristics that will be used by the automated employment decision tool. Violations of the provisions of the bill would be subject to a civil penalty. Read Local Law 144 of 2021.

Note: DCWP will begin enforcement of this law and rule on July 5, 2023.

We welcome the bill and consider it sends a signal to support responsible use of automated systems in the field of employment. This is of course with the understanding that this bill regards automated systems, which by default suggests a high risk.

Our understanding is that, following request for comments from the public, which included employers, a change has been introduced in the bill so that the auditor leading the bias audit of the system may exclude from this audit “a category that represents less than 2% of the data being used for the bias audit from the required calculations for impact ratio”.

We believe that this changed provision may open the door to significant risks of discrimination, and the fact that such exclusion would have to be justified by the auditor does not, in our opinion, bring sufficient safeguards.

Excluding a category representing 2% of data can:

- hide or hinder proper understanding of a bias that regards a minority group corresponding to a characteristic such as race, national origin, religion, etc.
- hide or hinder proper understanding of a bias that regards a group not frequently seen or considered in applications, eg. unemployed, long term unemployed or whistleblowers, who might be screened out from the earliest stages of the automated decision making and no easily noticeable as not tracked in the same way as protected characteristics;
- a 2% bias affecting a category could also reveal in fact the “tip of the iceberg” of a product flaw generating in fact a broader bias or risk of discrimination
- it gives also a non negligible discretionary power to system auditors who may be exposed to various level of pressure.

These remarks lead us directly to the known bias or discrimination against the unemployed.
**B°) Known bias or discrimination against the unemployed, including long-term**

The bias from recruiter and employers against the unemployed is not new and a known factor in the hardship experienced by numerous job seekers even when jobs suitable for their profiles are available.

Such bias or discrimination is harming communities, even more those who are the most exposed to economic hardship or unemployed, and initiates a vicious circle which, if not quickly interrupted, leads people to long-term unemployed which is often presented as an objective reason to reject an application.

Back in 2011, during the tenure of the Obama – Biden Administration, attempts were made to protect the unemployed by law, in order to make unemployment an additional protected characteristic.  
[https://www.huffpost.com/entry/obama-jobs-plan-bridge-to-work-program-long-term-unemployed_n_953838](https://www.huffpost.com/entry/obama-jobs-plan-bridge-to-work-program-long-term-unemployed_n_953838)

This effort was strongly by some business groups, and a new initiative to support the long-term unemployed was put forward by the Obama – Biden Administration in 2014, which succeeded to put in place a voluntary pledge from many companies to support the initiative.  

The main points here are:

- there is a persistent bias and discrimination against the unemployed when they apply ;
- this bias, if not quickly interrupted, automatically leads to long-term unemployment and hardship of those deprived of work ;
- **this kind of discrimination or bias is very easily set in automated employment decision tools** : eg. resumes / cv’s showing a gap after the last identified work position can be screened out after “x” weeks or months, or even immediately.

This bias can be openly noticed in recruitment forms asking for availability for candidates, that don’t include an option such as “immediately available” or “available now”.

We believe that this criteria should be scrutinized in AEDT, as this bias harm the rights of workers, increase the costs of unemployment while not bringing evidence that unemployed candidates would be less productive or efficient that those in jobs.

27 weeks is a short time span in the life of a business, even if that business is an AI vendor. 27 weeks is also the duration after which an unemployed person is considered as a long-term unemployed. Especially in the current economic context, we believe that there is an urgency to ensure that AEDT and other automated workers surveillance and monitoring systems don’t discriminate against the unemployed people, as more and more are just a few paychecks away from financial hardship, which can be another obstacle to get in employment.
Known bias or discrimination against financially underserved communities – example to access cyber jobs in ISO 27002

Performing a credit check can be part of many employment decision-making processes and this can be understandable in a number of situations. However, as many “screening” steps get automated and often without the required transparency and openness towards applicants, it can nullify in practice the recommendations or rights to know any adverse or negative information. https://consumer.ftc.gov/articles/employer-background-checks-your-rights https://www.ftc.gov/business-guidance/resources/background-checks-what-employers-need-know

To take an example, performing a credit check is explicitly mentioned in the standard ISO 27002 in the section pertaining to HR the hiring of cybersecurity professionals. The reasoning behind the requirement seems to be that adverse information in a credit report would either reveal lack of professional skills or present a risk for corruption or for bribery. What this assumption may not be always wrong, we believe it is strongly bias against underserved communities as it suggests a strong link between financial prosperity of an individual and his or her integrity. Cases when massive fraud, bribery or corruption was committed by wealthy individuals are not exceptions.

And just as for unemployed people, this process creates a vicious circle where people in financial hardship get refused access to employment, while getting employment would in fact resolve their hardship and put them on the way to prosperity.

As with the bias or discrimination against the unemployed, we believe automated credit check or similar automated steps – which may in reality be mere outdated information made available through data brokers but that is still regarded as current or genuine – create high risk for discrimination, go against policies such as the one to support Americans to get access to “high-quality, well-paying jobs, including jobs with opportunities to organize and bargain collectively with their employers through labor unions, as articulated in the Executive Order 14025 (Worker Organizing and Empowerment) 6 and through a competitive market for their labor, as articulated in Executive Order 14036 (Promoting Competition in the American Economy)”.

We believe that addressing this bias or discrimination based on financial situation in automated systems would be in the public interest, to support the above policies and it seems especially relevant in professions such as in cybersecurity where there is a strategic and urgent need to recruit.


US-UK Data bridge & potential risk of automated blacklisting via the CIFAS EIFD

The very recent announcement of the US – UK Data Bridge opens new opportunities for business between the two countries bound by the special relationship. The data transfer are
essential to many industries and we would like to raise here awareness about a specific that fits within the scope of this RFI.

Without making a call on respective qualities of data protection and privacy regulation in different countries and on other legislation applicable in the context of international data transfer – which is very broad and complex, it is reasonable to state that there may be a tendency among businesses to outsource remotely the provision of services they may know as questionable or even illegal, as an implicit obstacle to the exercise of worker’s rights.

As such, “screening” services mentioned in privacy policies are not only defined vaguely in terms of scope, but also in terms of location. For workers with limited financial resources and network, accessing legal advice oversees is indeed an obstacle.

Having taken the above under consideration, we believe that an increased flow of personal data can enable more remote “screening” services, including automated ones, and in this context, there is a significant risk if US based recruiters or employers access the CIFAS EIFD.

The EIFD is a specific database hosted by the CIFAS, which had previously a mission against fraud in financial services (National Fraud Database) or other databases that we do not address here. The Enhanced Internal Fraud Database is supposed to fight organized fraud, while according to CIFAS own staff, 80% of records are not related to that kind of fraud. This database has been extended to include now “employment application fraud”, and an inaccurate resume / cv is enough to get a record as a “fraudster”. Markers are kept for six years and having a record means that applications get rejected, without any hearing or cross examination.

As additional information, we are providing the following URLs:

- the CIFAS EIFD presented itself as a “benefit” to its members
  https://www.cifas.org.uk/fraud-prevention-community/member-benefits/data/ifd

- the list of CIFAS EIFD members
  https://www.cifas.org.uk/services/internal-fraud-database/internal-fraud-database-members

- an article published by a legal UK firm mentioning the misuse of CIFAS by employers
  https://www.msbsolicitors.co.uk/our-expertise/commercial/cifas-marker-removal/

- as a matter of comparison, we add the link to the “Violation tracker”, a research project based in the United States and tracking violations committed by corporations and their leadership – although those serious violations seem not being tracked in automated verification systems described above in C°) and in this section D°).
  https://violationtracker.goodjobsfirst.org/

We believe that the use of such so-called “internal fraud” service by automated worker surveillance and management systems would cause a high risk to workers’ rights, via a blacklisting system not providing genuine safeguards such as a right to be heard or even informed in the 80% of case that are not linked to the organized fraud it is supposed to tackle.
E° DoJ recent no-poaching case in Connecticut and the concept of buyers’ cartel in competition law

This subject is a very complex topic, and the court decision recently taken shows the enormous work done by the Department of Justice. While we do not claim knowledge in the field of US competition law, we would like to share the following with regards to the decision taken on 28 April by the District court of Connecticut, under No. 3:21-cr-220 (VAB), as it may related to organized labor discrimination outlined in part I°) of the present contribution and also in other settings.

The decision taken in this case has been summarized in a media as:

a°) The DoJ argued that the rule of reason didn't apply in this case because the no-poach agreement constituted a horizontal market allocation, where competitors at the same market level structure a labor market in order to minimize competition. However, the corporate executives said it wasn't a horizontal market allocation because it involved a vertical commercial relationship between the manufacturer and its outsourced providers.

b°) The court concluded the no-poach agreement was not illegal because the hiring restrictions frequently changed and allowed for exceptions, which suggests that often hiring was permitted, sometimes on a broad scale. "No reasonable juror could conclude that there was a cessation of meaningful competition," the court stated.

From a high-level reading of the decision, we understand the case as presented by the DoJ, and notice where the defendants appear to be circumventing the real issue which actually seems to be an horizontal cartel, as named by the DoJ, which act as a kind of buyers’ cartel, which is characterized in an OECD report titled “Purchasing Power and Buyers’ Cartels – Note by the European Union”, 22 June 2022 [Ref 9].

Page 8:
“According to the report, in the case of a buyer cartel, undertakings agree with one another on how they will individually interact with suppliers, or they exchange commercially sensitive information with one another about how they will individually deal with suppliers, thus removing competitive uncertainty that would otherwise have existed between them.”

Page 10:
“The distinguishing factor between a genuine purchasing agreement and a buyer cartel is whether the buyers, be it together or through a type of intermediary, collectively negotiate and conclude an agreement with a supplier. Conversely, if each buyer interacts individually with a supplier while coordinating its behaviour with other buyers, for example on their price negotiation strategy or through exchanges on the status of their individual negotiations, this amounts to a buyer cartel. In other words, the distinguishing factor is whether buyers present themselves jointly to a supplier in their negotiations or purchases or whether they seemingly act individually but nevertheless coordinate their behaviour with other buyers.”
If the same competition practices may be applicable to a buyers’ cartel interacting with suppliers as well as to an employers’ cartel interacting with employees, could we imply that:

- a vertical relation doesn’t exclude the existence of a horizontal cartel in its frame;
- the decision shows that the competitive uncertainty between employers has been removed;
- the employers interact individually with the employees while coordinating with other employers”.

This kind of process is, we believe, precisely what is impacting workers’ rights as shown in 1°).

F°) US law makers raising questions to data broker

In this section, we are sharing the information read in the press about an initiative taken by US law makers to bring more transparency about what happens in the data broker industry.

Data shared, sold or provided to third parties by any other mean could also be used as inputs, or received inputs, aggregated or not, from automated worker surveillance or monitoring systems.

The following URLs provide a press article and the full letter sent to one of these data brokers.


https://d1dth6e84htgma.cloudfront.net/05_10_2023_Acxiom_Data_Brokers_Letter_1cbb81da32.pdf?updated_at=2023-05-10T16:19:56.031Z

We believe that the 15 first questions could be also helpful to address the matters related to automated worker surveillance and monitoring systems, and we look forward, hopefully, to reading in the media the answers sent by these data brokers in response to the concerns raised by the US law makers on data protection & privacy of citizens.
IV°) Policies, practices, or standards that could protect workers (RFI section 4)

A°) Foreword: the five principles of the blueprint for an AI Bill of Rights

The AI Bill of Rights introduces five principles:

1. Safe and effective systems
2. Algorithmic discrimination protections
3. Data privacy
4. Notice and explanation
5. Human alternatives, consideration, and fallback

We believe that these principles provide a powerful yet accessible framework to scope and address major areas pertaining to AI and, whenever possible, we will use these principles as goals of the suggested policies, practices or standards that could protect workers. We realize how

B°) Thoughts about policies, practices or standards that could protect workers

a. What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers’ rights?

- As far as violations of labor market are concerned, in terms of competition, we believe the following resources about labor market agreements and competition policy by the Portuguese Competition Authority might be useful when considering practices “imported” to the United States from the EU and that can harm worker rights here too.

   Best Practices In preventing Anti-competitive Agreements in Labor Markets

- Items listed in below question “c” – a) regulation: may also be translated into standards or guidelines to assist vendors, employers or recruiters to comply with the proposed regulation.

b. Are there policy approaches to regulating automated worker surveillance and management systems from State, Tribal, territorial, or local governments or other countries that Federal agencies could learn from?

- we believe that the right of workers, as defined in the Universal Declaration of Human Rights, provide an overarching reference that may be easy to use and powerful at the same time to regulate what these automated systems may or may not do:
- there is a *Fundamental Rights Impact Assessment* developed in the Netherlands which provides a very detailed and practical framework to ensure responsible AI, which could also be used as an input or best practice to be considered when regulation such automated systems.

*Fundamental Rights and Algorithms Impact Assessment (FRAIA) | Report | Government.nl*

c. What policies or actions should Federal agencies consider to protect workers’ rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

a) regulations

These suggestions may address some of the risks or breaches presented in I°), II°) and III°)

- As discussed in III°) A°), we believe that fixed thresholds accepting a given level of bias, as the 2% bias tolerated in the NYC AEDT bill, may cause significant risks to minorities, protected categories or categories at risk of discrimination but not protected (unemployed, long-term unemployed, whistle blowers) of being discriminated, with automated, repeated and incremental harm that could quickly lead impacted people into dire hardship;

- As discussed in III°) B°), we believe that automated system, especially those taking decisions about access to employment (“screening”, “vetting”, ATS review, cv “verification”) should be scrutinized to ensure they don’t act as firewalls blocking access to work against the unemployed

- As shown in III°) C°), ISO standards such as ISO 27002 in cybersecurity may be broadcasting the idea of credit checks as a panacea for recruitment, we believe such standards could be reviewed on that matter, to a°) remove this recommendation when it is not absolutely required and/or b°) remind or specify what credit check results actually means and remind the right to a hearing, as outlined by the FTC since 2014.

- In Privacy notices, all these automated systems should be explicitly named and their work presented in terms that are fully understandable to the intended audience;

- We think that consent should not be admissible as a legal basis to collect or process PII in the context of work application, including when workers apply for new positions with their current employers

- forbid data sharing of applications made by a natural person with other recipients than the recruiter or the employer recruiting for that specific employment opportunity;

- forbid “digital pillorys” where employers or recruiters may comment cvs or profiles of candidate in front of other recruiters or employers, but without knowledge of the workers;

- demand that any cv, diploma or other verification automated systems be brought to the attention of candidates so that they may have a chance to be heard about any potential discrepancy (FTC’s “right of hearing”)
– right to access & rectify inaccurate employment related personal data / PII, within time lines that are shorter than the time when a persons becomes long-term unemployed which is used as a pretext by employers not to hire;

b) enforcement

- create a system or process of enforcement, with a speed and level of fines that provides dissuasion to dishonest employers, which would also bring an to honest or compliant ones;

- [unsure if this item should be in the “enforcement” or “regulation” as it could match either or both categories] The United States took a number of initiatives to reinforce cybersecurity and resilience, such as the initiative to improve the software supply chain:

  Link to the Executive Order: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

  Link to online form from CISA: https://www.cisa.gov/secure-software-attestation-form

We believe that this kind of approach applied to the ecosystem of automated worker surveillance & management systems would help to support Executive Order 14025 (Worker Organizing and Empowerment) and through a competitive market for their labor, as articulated in Executive Order 14036 (Promoting Competition in the American Economy)” in order to realize the awaited benefits for the public good.

Getting interfaces with vendors, employers or recruiters might also be facilitated by introducing a solution similar to the security file:

  security.txt: Proposed standard for defining security policies (securitytxt.org)

For instance, the above steps would help prevent threat and risks to the plan issued by the FTC to address abusive use of no-poaching agreements and the 300 billions USD lost for the US economy and prosperity.

c) grantmaking

- we believe that grantmaking could support independent research projects, which would be helpful to accelerate the discovery of the ecosystem and practices in terms of data sharing and automated systems.

Since March 2021, we have made an initial proposal for a research project proposed in Europe titled “Employment Data and Challenges to Individuals’ Privacy Rights”, which could assist in addressing the sources and scale of risks to workers rights, as well as identify potential solutions.

Overall, one of the priority would be to establish an inventory or observatory to stay on top of emergence of solutions, and ensure or anticipate needed rules, regulation pr guidelines be ready. Further information can be shared upon request.
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0155
Comment on FR Doc # 2023-09353

Submitter Information

Name: Heather Touhey
Address:
Email: [REDACTED]
Phone: [REDACTED]

General Comment

See attached file(s)

Attachments

RFI Automated Worker Surveillance and Management
Response to: Request for Information: Automated Worker Surveillance and Management

The White House Office of Science and Technology Policy (OSTP)

From: Heather Touhey
CEO of Tsunami Solutions

June 13, 2023

Dear Office of Science and Technology Policy,

As the CEO of Tsunami Solutions, our mission is to “use innovative and user-centric technology to solve health, safety, and security challenges that people face every day”. We have diligently worked to develop robust and efficient systems designed for the improvement of health and safety in workplaces, with a keen focus on lone worker safety. Our primary product, SafetyLine Lone Worker, has successfully monitored the safety of thousands of lone workers in multiple industries across the globe, assuring their safe return to their loved ones each day.

My passion for ensuring workplace safety was ignited during my tenure as an occupational therapist. Witnessing the devastating aftermath of workplace accidents, especially to other healthcare workers and their families, I was inspired to shift from reaction to prevention. SafetyLine is particularly well suited at the healthcare sector, where I have witnessed a pressing need for effective safety measures. I bring to this discussion not only my experience as the CEO of Tsunami Solutions but also my unique insights as a healthcare professional, a scientist, and a doctoral candidate at Boston University.

In response to the Request for Information (RFI) from the White House Office of Science and Technology Policy (OSTP), I write to bring attention to a critical aspect of automated worker surveillance and management. While the focus of the RFI is understanding potential risks to workers’ rights, opportunities, access, health, or safety, it is equally important to recognize the protective role of certain types of surveillance systems. Specifically, I want to shed light on the lifesaving potential of lone worker monitoring systems.
Lone Worker Legislation

The prominence of lone worker legislation in developed nations worldwide underscores the importance of safeguarding workers who function beyond the sight and immediate help of their colleagues. The United States has no specific legislation aimed at protecting its lone workers, instead often leaning on the General Duty Clause to address lone worker safety as seen after an employee death at North Suffolk Mental Health Association. While the clause is valuable, it lacks the precision and comprehensiveness of dedicated lone-worker legislation. This is an opportunity for the United States to join other global communities and demonstrate leadership in lone worker safety and protection.

Health Care Industry Violence in the Workplace against marginalized populations

An unsettling reality we must confront is the disproportionate lack of occupational health and safety technology for workers in industries such as healthcare and social services, which are often staffed predominantly by marginalized and vulnerable populations. According to research conducted by PHI, 87% of home care providers are female, 62% are non-white, only 20% have an associate degree or higher and have a mean annual earning of $16,200 placing them well below the poverty index. (Scales, 2020). Additionally, according to the US Bureau of Labor Statistics “in 2022, persons with a disability were more likely to work in service occupations than were those with no disability” (Statistics, 2021) and are well represented within the healthcare field.

What is more significant is the amount of violence in the workplace and violent death is substantially higher in this occupation. Between 2011 and 2013, there was an average of 24,000 assaults per year, where 75% occurred within the health care setting. The Bureau of Labor Statistics found that healthcare workers are four times more likely to require time away from work due to injury from violence. Of particular note is the uniquely higher risks seen amongst home health care workers. Approximately 61% of home healthcare workers report incidences of violence annually (Hanson, 2015). Most notably, homicide is the leading cause of workplace death in this demographic, second only to motor vehicle accidents. Finally, it should be noted that estimates show that only between 3 and 6.5% of workplace violence events against health care workers are reported, indicating that this is an even bigger problem than originally reported (Copeland, 2017) (Arnetz JE, 2015). The OSHA Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers clearly highlight "Working alone in a facility or in patients’ homes" and "Lack of means of emergency communication" as risk factors contributing to this surge in workplace violence (Occupational Safety and Health Administration, 2016). Despite these glaring risks, the absence of adequate legislative protection for these lone workers continues.

Lone Worker Legislation as Discrimination

In contrast, OSHA provides distinct lone worker guidelines for other industries, such as Underground Construction (29 CFR 1926.800), Longshore work (1917.30), and Shipyard operation (1915.84), which typically register lower rates of workplace violence and are less comprised of marginalized populations. These legislations cover various safety aspects, including emergency communication, training, and check-in/check-out procedures, ensuring the accountability and safety of every worker.
While commended for the inclusion of lone worker legislation within certain industries, the absence of such safeguards as lone worker legislation for the healthcare industry which is primarily supported by marginalized groups, not only speaks to discrimination but also stands in violation of the mandates set by Title VII of the Civil Rights Act of 1964, Title I of the Americans with Disabilities Act of 1990, and Sections 501 and 505 of the Rehabilitation Act of 1973. The absence of equal protection is not just a matter of workplace safety—it also raises serious legal and ethical concerns. These legislations are not a luxury; rather, they are a fundamental right that all workers should be granted equally. However, it is strikingly apparent that this right is not uniformly distributed.

**Domestic and International lessons on Lone Worker Safety**

While the legislation provided to other industries has been a positive move forward, the healthcare industry has been omitted and requires dire attention. The 2022 Surgeon General Report on Health Worker Burnout states:

“Protecting health workers from workplace violence must be prioritized by all institutions and communities and must be supported by legislation. Health systems must ensure that health workers are adequately trained for all scenarios and provided with a robust supply of personal protective equipment.” (Medicine, 2020)

To bridge this gap in legislation, lessons can be drawn from countries with successful lone-worker legislations such as Canada, the UK, and Australia, where specific laws mandate employers to adopt systems ensuring lone-worker safety. Although each is unique, they all entail provisions for risk assessment, safety measures, training and documentation, emergency response plans, and crucially, check-in/check-out procedures.

At the core of an employee monitoring solution for lone workers, is a proactive check-in system, not just a cell phone or a panic button. A pro-active check-in system, when implemented correctly, can reduce the time it takes to respond to an emergency, potentially saving lives. We can refer to a slew of standards and regulations worldwide that hold high levels of security and privacy to prevent misuse of these systems for productivity management, such as the UK’s BS8484 Regulations (INSTITUTION, 2022).

Renowned companies providing lone worker safety solutions have successfully adhered to these regulations. For example, AlertMedia, an organization based out of Austin Texas, is a market leader in providing worker safety monitoring. They offer a suite of wirelessly connected products that deliver a high standard of worker safety through monitoring, real-time situational awareness, and a set of advanced reporting tools.

At Tsunami Solutions, our SafetyLine Lone Worker monitoring system is designed to respect user privacy while providing a safety net that calls for help when the worker cant. Our service ensures real-time check-ins, efficient location tracking, and swift emergency response, thereby mitigating workplace safety risks. Concerns surrounding misuse of data and security are alleviated by SOC II Type 2 certification and offset by increased safety. A poignant success story of our system’s efficacy is our partnership with Seasons Consulting Group, where our solution has significantly improved their lone worker safety and overall workplace health and safety practices.
**Recommendations**

With the current focus on supporting the healthcare industry through workplace safety, healthcare violence, and discrimination, it is paramount that the U.S. adopts a comprehensive federal lone worker safety legislation. This legislation should be cognizant of marginalized worker populations’ needs and should provide equal protection to all, irrespective of their roles or the industries they work in.

The implementation of proactive, privacy-preserving lone worker monitoring systems would ensure safer work conditions, protect workers’ rights, and support justice not only in the healthcare sector but in all industries.

In conclusion, it’s time we stopped seeing lone worker monitoring as an issue of surveillance and started seeing it as a tool for ensuring equality in access to safe workplaces. We must harness the power of technology to create a safer, more inclusive workplace for all, where safety rights are universally recognized and respected, regardless of industry or demographic representation.

Sincerely,

Heather Touhey, BSc, MOT, OTD Candidate.
References


PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0156
Comment on FR Doc # 2023-09353

Submitter Information

Email: National Treasury Employees Union

General Comment

See attached file(s)

Attachments

Alan Mislove re OSTP RFI Comments
June 15, 2023

VIA FEDERAL eRULEMAKING PORTAL (http://regulations.gov)

Dr. Alan Mislove  
Assistant Director for Data and Democracy  
Office of Science and Technology Policy  
Executive Office of the President  
1650 Pennsylvania Avenue, N.W.  
Washington, D.C. 20504

RE: Request for Information; Automated Worker Surveillance and Management

Dear Dr. Mislove:

The National Treasury Employees Union (NTEU) submits these comments in response to the notice published in the Federal Register on May 3, 2023 (88 Fed. Reg. 27,932) (RFI), in which the Office of Science and Technology Policy (OSTP) invited comments from stakeholders—including labor unions—regarding automated worker surveillance and management (AWSM). NTEU is the exclusive representative of federal employees in 34 departments and agencies.

On behalf of the thousands of federal workers we represent, NTEU urges the Executive Branch to carefully consider all angles of AWSM both as a regulator and as an employer. The federal government has an opportunity to lead the way on these issues, especially given its commitment to acting as “a model [employer] that sets an example for other private and public sector employers in America and around the world.”1 Because both public- and private-sector employers are embracing AWSM tools at such a rapid pace, the example the government sets may be even more important than the rules it eventually adopts.

As one of the largest federal labor unions, NTEU’s perspective is critical in the ongoing conversation about AWSM—especially when the government uses these tools to manage its own workers. These comments focus first on the IRS’s use of employee monitoring tools at taxpayer service centers across the country. Second, these comments discuss the myriad ways that AWSM can create, amplify, and disguise bias in the workplace. Finally, these comments highlight key policy considerations that the government should prioritize when it regulates other employers’ use of these tools—and when it uses such tools itself.

I. NTEU has negotiated key protections for employees subject to surveillance and automated monitoring at IRS Taxpayer Service Centers.

NTEU represents IRS customer service representatives who assist taxpayers at service centers around the country. The safeguards NTEU has negotiated for employees subject to surveillance and automated monitoring serve as helpful examples for policymaking in this space.

As part of their job-appraisal system, the agency records employees’ telephone calls with taxpayers. Before the IRS can use any recording of an employee to evaluate performance, it must alert the employee within three weeks after the recording occurred. The employee is entitled to an opportunity to listen to the recording and rebut the agency’s interpretation. Further, recordings are routinely deleted after approximately 40 days. Thus, employees have access to any data the agency proposes to use to support a negative performance appraisal. They have the right to listen themselves and respond. The agency must act promptly on any recordings it flags, and recordings are routinely deleted when they reach a certain age. These are important protections for employees subject to this type of monitoring.

Many service center employees are also subject to an automated performance appraisal system that measures quality and efficiency. NTEU has negotiated with the agency to ensure employees’ and union access to the performance reports generated by the system. The agency must negotiate with the union any time that it wishes to change the performance standards used by the system.

Finally, the IRS uses an automated time tracking system for employees who handle taxpayer telephone calls. Employees subject to this system are entitled to review their written time reports and raise any inaccuracies with their managers.

The common thread here is employees’ access to their own data combined with the chance to raise any inaccuracies, needed corrections, or additional information. NTEU has negotiated these employee protections to ensure that the IRS’s use of these surveillance and monitoring systems is transparent and equitable. As discussed further below, policymakers should consider rules that prioritize transparency and accountability whenever employers use automated systems to surveil or otherwise monitor their employees.

II. The government must guard against AWSM tools that create, amplify, or disguise bias.

NTEU urges OSTP and other policymakers to carefully consider measures to mitigate the harm AWSM can inflict by creating, disguising, or amplifying conscious and unconscious bias. These dangers exist at every stage of the employment relationship. While automated hiring and screening systems are sometimes touted as “objective” because they remove human judgment, these tools are created by humans, are not objective, and indeed, incorporate the existing biases present in us all. Even if biases are not reflected in the initial dataset, automated hiring tools can
yield unforeseen disparate impacts on protected and underrepresented groups. Moreover, when automated tools are used to analyze far more data than humans can on their own, the biases inherent in the tools may be even further amplified. Policymakers must ensure that employers cannot disguise bias and discrimination with automated tools, leaving job applicants and employees worse off.

Automated management tools can foster bias and discrimination against many protected and underrepresented groups, which in turn may create serious setbacks for employers’ diversity, equity, and inclusion goals—not to mention the risk of violating existing anti-discrimination law. For example, some facial recognition systems used by employers have performed worse when scanning employees of color. When AWSM tools evaluate employees based on their proficiency with technological tools, they may discriminate based on age and/or disability. And with enhanced access to data on applicants and employees, AWSM tools can make predictions or other assessments that can easily lead to discrimination. For instance, around ten years ago Target used consumer data to predict pregnancies in individual customers. The more data employers collect about their employees, the more likely the employers are to discriminate against employees, whether intentionally or not.

Avoiding express reliance on protected characteristics is not enough. Screening methods that appear legitimate and objective on the surface can function as proxies for protected characteristics. Examples include names coded to a certain race or nationality and zip codes that disproportionately screen out members of specific groups during the hiring process. The government and employers alike must actively guard against these biases as AWSM tools become more prevalent.

---


3 See Danielle Abril & Drew Harwell, Keystroke tracking, screenshots, and facial recognition: The boss may be watching long after the pandemic ends, WASH. POST (Sept. 24, 2021), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/ ("[S]ome facial recognition systems have been shown in research to perform worse with people of color because the algorithms are less accurate at identifying people with darker skin tones.").


5 Kim & Bodie, supra note 2, at 312 n.137.

6 Id. at 294.

7 Id.
III. The government should create policies that protect employees against potential pitfalls and abuses created by automated surveillance and management tools.

NTEU urges the administration to keep the following key considerations in mind when it regulates employers’ use of AWSM.

A. Transparency

Transparency around how the employer uses AWSM is essential to protect employees. In this context, “transparency” includes disclosure of what AWSM tools are being used, clarity about how they are used, and employees’ access to their own data. Requiring disclosure and access to data can mitigate power imbalances that occur when employers retain exclusive access to large volumes of data used for—and produced by—AWSM tools. Existing laws in some cities, states, and other countries promote transparency, but on the whole current U.S. law is woefully inadequate.

New York City recently enacted a law governing employers’ use of artificial intelligence in hiring and promotion. If an employer chooses to use an “automated employment decision tool,” it must disclose its use of that tool to internal and external candidates for a position.\(^8\) Upon request, the employer must also provide the candidate or employee with “information about the type of data collected for the automated employment decision tool, the source of such data and the employer or employment agency’s data retention policy.”\(^9\) A few states, including California, Connecticut, and Delaware, also require employers to notify their employees about any electronic monitoring in the workplace.\(^10\)

NTEU has proactively negotiated surveillance transparency protections in some of its contracts, including its collective bargaining agreement (CBA) with the IRS. The contract requires the agency to provide NTEU with notice and the opportunity to bargain if the agency decides to use covert video surveillance or monitor employees’ email. The CBA further requires the agency to provide any evidence derived from phone monitoring to employees when the evidence is used as support for a proposed disciplinary or adverse action.

The European Union’s (EU) regulatory approach to AWSM tools also prioritizes transparency. EU rules require the subjects of personal data processing to be informed about the categories of data collected, the purpose of the processing, how the data will be used, and how subjects can challenge the use of their data.\(^11\) The rules go even further by giving subjects the

---

\(^8\) N.Y. City Admin. Code § 20-871(b)(1).
\(^9\) Id. at (b)(3).
\(^10\) Kim & Bodie, supra note 2, at 305.
\(^11\) Id. at 311.
right to “correct inaccurate data,” “supplement incomplete data,” and “request deletion of data under some circumstances.”

On the flip side, most U.S. states do not require employers to disclose their use of AWSM tools. As EU rules around informed consent recognize, by its nature the employer-employee relationship involves a major power imbalance between an employer and its workers. Policymakers should seek to mitigate the impact of this asymmetry when regulating AWSM. Just as provided by EU regulations and some NTEU contracts, employers should be required to allow employees to access their own data in appropriate circumstances—especially when it is used to justify disciplinary action. Transparency must be the foundation of any AWSM regulatory regime.

B. Accountability

Transparency is the starting point, but it is not enough on its own. Employers, including the federal government, must also be held accountable for their use of AWSM tools. They must not be able to hide behind the fact that their AWSM tools constitute a “black box” that even they do not understand. Instead, employers should be able to explain how they use AWSM and how the tools affect their employment decisions. Because employers are the ones who choose when and how to implement these technologies, the burden should be on them to establish that they are using AWSM tools legally, responsibly, and ethically.

In the federal employment context, the existing legal framework already places the burden upon the federal government to provide more than the output of AWSM monitoring when using AWSM in its decisionmaking as an employer. For example, NTEU uses information requests under 5 U.S.C. § 7114(b)(4) to gather information from agency-employers during disciplinary proceedings and grievances. When these information requests include data from AWSM tools, NTEU, as well as neutral factfinders adjudicating these proceedings, will not be satisfied with only the end result. Whether AWSM is involved or not, the government must be able to explain the reasoning it uses to arrive at its decision. Employers, including federal agencies, should not be permitted to escape this burden by using AWSM. Without accountability, it is impossible to meaningfully enforce existing and future worker protections developed to regulate these tools.

---

12 Id.
13 See id. at 305.
14 Id. at 310.
15 See, e.g., 5 U.S.C. § 7513(b)(1) (providing that agencies are required by law to provide written notice, with “specific reasons,” when it plans to discipline an employee). See also Lachance v. Devall, 178 F.3d 1246, 1257–58 (Fed. Cir. 1999) (“Absent the articulation of specific reasons, agency action is ineffective as it does not comply with statutory requirements.”).
C. Employee Privacy

Consumer privacy and the collection of personal data are frequently discussed topics in the media and elsewhere. However, the implications of employers collecting personal data about their employees are not discussed as frequently. The potential for abuse may be even greater in the latter context. Workers are typically in long-term relationships with their employers, who have immense power over their pay; their working conditions; and, ultimately, their daily lives, health, and wellbeing.

Protecting employee privacy is paramount, especially because AWSM tools enable employers to collect and analyze data at greater speeds and in greater quantities than humans could ever accomplish. Policymakers must consider whether current legal frameworks adequately regulate such use of employees’ data. Even if employers do not have nefarious intentions, they should not be left to self-regulate in this space given their incentives to streamline, save money, and increase efficiency. The path of least resistance will often create unjustified risks for employee privacy. Accordingly, policymakers must step in to protect employees’ rights.

The more data employers have, the greater the privacy risks. Under the “mosaic theory” of data collection, “the whole is greater than the sum of its parts.”16 As in the Target example discussed above, with enough data automated tools can predict pregnancies and infer other details about employees’ lives. The more data employers collect, the greater the privacy and discrimination risks. Any regulations of AWSM must strive to protect employee privacy.

For the federal workers that NTEU represents, the Fourth Amendment also comes into play in the workplace. While NTEU believes that all workers’ privacy should be carefully protected, we emphasize here that “[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer.”17

As the Supreme Court has explained, courts must proceed cautiously “when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer.”18 The Court has declined to outline a broadly applicable test regarding workplace privacy expectations precisely because “[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”19

---

19 Id. See also Bowers v. Cty. of Taylor, 598 F. Supp. 3d 719, 726 (W.D. Wis. 2022) (quoting O’Connor, 480 U.S. at 718) (reiterating Supreme Court’s caution that “[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis”).
Indeed, this area of Fourth Amendment law is “largely unsettled.” But recent case law has illustrated a few potential applications of the Fourth Amendment to automated employee monitoring. For instance, searches conducted for improper purposes or through means that are “too intrusive,” including those that collect large quantities of data, may violate the Fourth Amendment. And the increasing prevalence of telework—including frequent use of computer cameras and audio devices—implicates the location where employees have the greatest expectation of privacy: their homes. When employers use AWSM tools that intrude upon the home, they risk violating their employees’ constitutional rights. As an employer, the government must structure any use of AWSM tools to avoid such violations.

For these reasons, the government should keep privacy concerns at the forefront as it navigates the AWSM legal landscape, both as a regulator and as an employer.

* * *

Thank you for the opportunity to submit comments on this important topic. Please do not hesitate to contact NTEU for elaboration of these views.

Sincerely,

Anthony M. Reardon
National President

---

20 Bowers, 598 F. Supp. 3d at 726 (observing lack of settled precedent regarding government employees’ expectations of privacy and individuals’ expectations of privacy in electronic data).

21 See, e.g., Larios v. Lumardi, 445 F. Supp. 3d 778, 783–85 (E.D. Cal. 2020) (finding that the amount of data seized when employer downloaded entire contents of employee’s personal phone “was vastly disproportionate to the amount of work product Defendants suspected to find” and that employer therefore “violated Plaintiff’s Fourth Amendment rights”).

22 See, e.g., Florida v. Jardines, 569 U.S. 1, 6 (2013) (“At the [Fourth] Amendment’s very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.”) (cleaned up).

23 See, e.g., Ogletree v. Cleveland State Univ., Case No. 1:21-cv-00500, 2022 U.S. Dist. LEXIS 150513, at *29 (N.D. Ohio Aug. 22, 2022) (finding that a student’s privacy interest within his home outweighed his university’s interest in using artificial intelligence and his computer’s camera to scan his room for suspicious activity during a remote exam).
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0157
Comment on FR Doc # 2023-09353

Submitter Information

Email: [REDACTED]
Organization: the Computer & Communications Industry Association (CCIA)

General Comment

CCIA Submits the following comments to the Office of Science and Technology Policy. See attached file(s)

Attachments

2023-06-15_CCIA Comments OSTP RFI on Automated Systems and Workers
COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Request for Information (“RFI”) published in the Federal Register at 88 Fed. Reg. 27932 (May 3, 2023), the Computer & Communications Industry Association (“CCIA”)\(^1\) submits the following comments to the Office of Science and Technology Policy (“OSTP”).

I. Introduction

CCIA is pleased to provide comments on how the federal government can facilitate and promote the responsible use and development of automated systems and tools in the field of employment. Automated systems and similar technologies have created tremendous benefits for employees and employers. Businesses in every industry sector use automated systems to improve their competitiveness and enhance their products and services, including routine and low-risk applications such as filtering and spell-check. During COVID-19, the use of automated systems has enabled individuals to work safely by helping employers utilize cameras, sensors, and augmented reality to create important social-distancing tools and enforce relevant health protocols.\(^2\)

---

1 CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

Automation has also increased organizational efficiency to provide employees with new opportunities to engage in more impactful work. However, at the same time, such technologies may pose risks to individuals if poorly developed and implemented, especially if organizations fail to account for important considerations like those around bias and fairness. The 1974 Equal Credit Opportunity Act sought to prevent discrimination in the lending market through the use of credit scores. But as studies have shown, numerous issues like flawed or incomplete data, have undermined this objective.

CCIA and its members appreciate the Administration’s commitment to providing workers access to high-quality, well-paying jobs. While CCIA shares the Administration’s concerns and agrees more work can and must be done to study the potential implications of automated systems and related technologies, we caution against any overly prescriptive approach to such technologies, especially concerning the use of low-risk technology. Further, the Administration’s recent adoption of the word “surveillance” in connection with new technologies is troubling. The word suggests a nefarious purpose, as well as intent to police or sanction individuals and employees, and a clandestine mode of operation. Most of all, “surveillance” connotes a violation of rights and thus appears to presuppose the existence of actionable harm. Using this word further attempts to undermine the progress and benefits associated with automated systems. CCIA encourages the federal government to reject the term “surveillance” as a divisive, inflammatory, and inapt term for all practices contemplated by this RFI. It would be more productive to distinguish between high- and low-risk uses of automated systems, aligning with emerging legislative approaches seen in the states and other jurisdictions. The Association appreciates the opportunity to further detail our experiences with automated systems, including the benefits created by these technologies and opportunities for the federal government to provide guidance, foster collaborations, and facilitate the sharing of best practices.

---


II. Benefits Created from the Use of Automated Systems and Related Technologies

The adoption of automated systems and AI across industries is widespread and growing. A 2022 McKinsey and Company study found that 56% of business leaders across the globe now report using AI in at least one business function.\(^6\) The report highlights that the most common AI use cases are low-risk, involving service-operations optimization, AI-based enhancement of products, and contact-center automation. These advancements have enabled small businesses to effectively market their products to the right consumers at affordable prices and allow for better customer experience and cheaper prices.\(^7\) Such automated systems have helped small businesses improve their efficiency and productivity, increase accuracy and reduced errors, and improve internal collaboration and communication.\(^8\)

The use of these technologies has yielded tremendous benefits for employers of all sizes and employees of all abilities, with online recruitment and job advertising, applicant screening, and qualitative assessments. These systems and tools have helped employers improve their hiring procedures and process, such as using AI-driven neuroscience games to assist in identifying new traits and considerations like emotion and generosity.\(^9\) Cost savings for organizations of all sizes enables resources to be allocated to other important interests and priorities beyond hiring, including diversity, equity, and inclusion initiatives.

In anticipation of this year’s U.S.-EU Trade and Technology Council meeting, the Administration released its economic study on the impact of AI on the future of workforces in the European Union and the U.S.\(^10\) The comprehensive report highlights the economics behind AI-driven technological change with a focus on the institutional and policy decisions that will shape its future impact on the workforce. Notably, the case study on the use of AI in Human Resources and Hiring concluded that “[t]he overarching message from discussions with firms in

---


the hiring space was that AI-powered algorithms could improve nearly every step in the hiring process for firms, HR staff members, and candidates.”11

With the United States still facing serious labor shortages in both the public and private sectors,12 the federal government has an opportunity to prioritize the advancements of these technologies for the betterment of workers and society. Current and future workforces will depend on a blend of using traditional hiring methods and automated employment decision tools.

III. Policies, Practices, and Standards

Innovation brings new opportunities with improvements to existing technologies and the creation of new tools. Despite these rapid advancements, the decisions and activities driven by automated systems and artificial intelligence are subject to Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, and other existing civil rights laws. In April, the Department of Justice’s Civil Rights Division, the Consumer Financial Protection Bureau, the Equal Employment Opportunity Commission, and the Federal Trade Commission all reaffirmed in a joint statement that “their existing legal authorities apply equally to the use of new technologies as they do to any other conduct. The joint statement summarizes recent accomplishments, including policy guidance and enforcement actions, the agencies have taken to combat illegal behavior committed through the use of automated systems.”13 These agencies have continued to use these existing authorities to enforce non-discrimination, consumer protection, and other important legal protections.

CCIA cautions against rushed attempts to regulate automated and AI systems, which are complex and warrant adequate understanding to reach intended outcomes appropriately. Any regulation of automated systems and decision-making technology should keep in mind that automated systems are a subset of decision-making — and so existing laws, including those

---

11 Id. at 29 (emphasis added).
13 See Press Release, Department of Justice, Justice Department’s Civil Rights Division Joins Officials from CFPB, EEOC and FTC Pledging to Confront Bias and Discrimination in Artificial Intelligence (Apr. 25, 2023), https://www.justice.gov/opa/pr/justice-department-s-civil-rights-division-joins-officials-cfpb-eecoc-and-ftc-pledging (“Our agencies reiterate our resolve to monitor the development and use of automated systems and promote responsible innovation. We also pledge to vigorously use our collective authorities to protect individuals’ rights regardless of whether legal violations occur through traditional means or advanced technologies”).
aforementioned, that govern how a company makes decisions generally would also apply to such automated systems.

Regarding laws targeted solely at automated systems, companies in the United States are subject to several existing state privacy laws that already impose substantial obligations concerning the individual right to opt-out of automated decision-making. This includes the Colorado, Connecticut, and Virginia state privacy laws. Critically, each of these laws is limited to high-risk decisions, described as those which have “legal or similarly significant effects,” and in the case of Connecticut, target “solely” automated decisions.

To ensure interoperability with those laws and to strike the right balance between protecting individuals while enabling access to important technology, the federal government should seek to align its approach by focusing on only those systems that (i) involve decisions with legal or similarly significant effects, (ii) are limited to solely or fully automated decisions, and (iii) apply only after an automated decision is made. Low-risk automated systems, such as GPS systems, spam filters, and driver monitoring, should not be the focus of any potential regulation. Organizations should not have to design objectively worse, and potentially even dangerous, versions of their products and services merely to give the individual the right to opt-out of the automated system. For example, Amazon’s use of its real time alerts for drivers has produced “remarkable safety improvements–accidents decreased 48 percent, stop sign violations decreased 20 percent, driving without a seatbelt decreased over 60 percent, and distracted driving decreased 45 percent.”

Furthermore, the regulatory focus should be limited to high-risk use cases, such as using technology to make final decisions regarding access to housing, credit, medical benefits, or other critical services without appropriate human involvement. Although organizations routinely use such automated systems to aid in employment decisions, such final decisions are still a result of human oversight and input. Importantly, responsible companies remain committed to the responsible use of advanced automated systems and similar technologies. Some examples include Meta’s five pillars of Responsible AI, AWS’s guide on the Responsible Use of Machine Learning, and Google’s Responsible AI practices. For example, AWS’s guide provides

---

considerations and recommendations for responsibly developing and using machine learning systems across three major phases of their life cycles: design and development; deployment; and ongoing use.

However, organizations could benefit from increased guidance and sharing of best practices which enable employers of all sizes to learn about important risks and considerations in using these tools. Expert agencies like OSTP can play a pivotal role in developing trustworthy automated systems and AI, which will require a comprehensive approach and extensive collaboration between all stakeholders. CCIA encourages the federal government to consider alternative non-regulatory approaches to policy issues affecting artificial intelligence applications, including enforcement guidance and sharing of frameworks and consensus standards. The Administration can look to the National Institute of Standards and Technology’s (“NIST”) AI Risk Management Framework, a voluntary and flexible framework that was the result of significant collaboration between government, industry, civil society, and other stakeholders. Additionally, the NIST AI Playbook helps organizations navigate and incorporate the Framework’s considerations like trustworthiness in the design, development, deployment, and use of AI systems. Industry and the advocacy community continue to collaborate on many of the difficult policy considerations relating to advanced systems, including fairness, transparency, the future of work, and economic impacts.

16 See Partnership on AI, which includes over 100 industry and advocacy members, conducting research and thought leadership to advance understanding of AI technologies, https://www.partnershiponai.org/.
IV. Conclusion

CCIA applauds the Administration’s commitment to encouraging the responsible use and development of automated systems and similar technologies.

Respectfully submitted,

Alvaro Marañón
Policy Counsel
Computer & Communications Industry Association

June 15, 2023
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0158
Comment on FR Doc # 2023-09353

Submitter Information

Email: [REDACTED]
Organization: Bipartisan Policy Center

General Comment

See attached file(s)

Attachments

BPC Response to OSTP RFI on Automated Worker Surveillance and Management
BY ELECTRONIC MAIL

Stacy Murphy
OSTP
1650 Pennsylvania Avenue NW
Eisenhower Executive Office Building
Washington, DC 20502

Re: Document 2023-09353: Bipartisan Policy Center Response to the Office of Science and Technology Policy Request for Information on Automated Worker Surveillance and Management

Ms. Murphy:

The Bipartisan Policy Center’s (BPC) Technology Project welcomes this opportunity to submit a response to the Office of Science and Technology Policy’s request for information on Automated Worker Surveillance and Management. As an organization committed to helping policymakers work across party lines to craft bipartisan solutions, we welcome OSTP’s effort to solicit information from the public, “on the prevalence, uses and purposes, and deployment of automated worker surveillance and management systems, including impacts of these systems on workers' legal rights and lives.”

BPC’s Technology Project supports efforts to prepare the workforce for the future and promote responsible, ethical, and trustworthy technology. Below, we provide information about BPC, the Technology Project, and our ongoing work to develop smart data governance practices. Finally, we offer policy recommendations to protect workers’ rights and privacy and promote ethical and responsible automated worker surveillance and management practices.

I. Introduction to Bipartisan Policy Center and the Technology Project

The Bipartisan Policy Center is a non-profit, 501(c)(3) organization that delivers data and context, negotiates policy details, and creates space for bipartisan collaboration so our democracy can function on behalf of all Americans. We leverage our relationships with current and former elected officials, business leaders, academics, and advocates across the political spectrum to shape practical policy ideas. What sets BPC apart from traditional think tanks is our unwavering view that engaging “proud partisans” is
essential to creating better solutions and solving our nation’s problems. We embrace the reality that good ideas alone do not drive policy change, and we have crafted the networks, policy expertise, and persuasion techniques to work around that fact.

BPC began its technology policy work in late 2019 with our initiative to develop a national AI strategy for Congress in collaboration with Former Rep. Will Hurd (R-TX) and Rep. Robin Kelly (D-IL). Through this initiative, BPC held a series of roundtables with government officials, industry representatives, civil society advocates, and academics. Subsequently, we produced four whitepapers on AI and the workforce, AI and national security, cementing U.S. AI leadership through research and development, and AI and ethics. These whitepapers provided several recommendations that H.Res.1250 incorporated.

Since then, we have continued our policy work in AI, consumer data privacy, and other data governance issues by educating Congress, analyzing policy proposals, and engaging with stakeholders. We continued our work on AI by publishing a report on the EU’s efforts to regulate AI. We also explored academic, government, civil society, and industry perspectives for policymakers to consider when crafting AI impact assessments. Most recently, BPC published pieces on defining high-risk, high-reward AI and workforce resilience and adaptability for the AI-driven economy. This week, BPC submitted comments in response to the National Telecommunications and Information Administration (NTIA) AI Accountability Policy Request for Comment (RFC). On data privacy issues, we have written blogs covering face recognition technology governance challenges, public sector data sharing and transparency reporting, and numerous white papers on state and federal actions to address consumer and children’s privacy and data protection regulations.

The Technology Project’s portfolio has expanded to include content moderation, immersive technologies (e.g., augmented reality and virtual reality), competition, cybersecurity, space, and broadband/digital divide policy issues. More information about these initiatives is available on our website.

II. Comments in Response to RFI Questions

A thriving U.S. economy is fueled by vast amounts of data and powerful tools that can effectively harness and process it. However, considering the widespread adoption of employee monitoring software and the many challenges presented in the RFI by other stakeholders on automated workplace surveillance technology, policymakers must explore comprehensive approaches that ensure businesses are prepared to implement safeguards to protect the public, especially vulnerable populations, and cultivate a resilient, skilled, and competitive workforce.

A thorough evaluation of existing laws and regulations is crucial to effectively address these concerns. This review should encompass data collection and privacy, civil rights and liberties, artificial intelligence (AI), and labor laws and regulations, in addition to general and sector-specific laws and regulations that could apply to various AI use cases. By reviewing existing federal, state, and local governance
frameworks; identifying gaps; and developing legislation, regulations, and/or non-legally binding best practice resources to help close gaps, policymakers can ensure that appropriate safeguards and protections are in place to protect individual rights and mitigate potential risks. We are pleased to share our considerations for automated surveillance and management in the workplace.

**a. Implications of automated worker surveillance and management (Questions 1-4)**

Different technologies have their own implications and considerations. For instance, face recognition technology raises questions about the collection and use of biometric data, potentially affecting worker privacy and security. Virtual reality and augmented reality technologies present unique challenges in terms of data collection and retention, as they create immersive experiences that may involve capturing sensitive behavioral information. On the contrary, the utilization of synthetic data and other privacy-enhancing technologies (PET) introduce new possibilities for safeguarding worker privacy while enabling useful data analysis.

BPC facilitated several discussions on the intersection of emerging technologies and their workplace implications with a range of stakeholders representing workers, employers, and developers. As the convener, BPC drew upon our experts’ perspectives and identified several overarching themes, including advantages and concerns related to automated monitoring systems, from these discussions. These themes form the basis of the insights we provide below.

i. **Potential Benefits**

The adoption of automated surveillance and monitoring systems may yield improvements in overall productivity, efficiency, and security of business operations, but more research is needed. By implementing monitoring processes, businesses can identify areas for optimization, monitor for fraud and theft, and refine their practices accordingly. This increased efficiency can lead to enhanced worker productivity and business functions.

Leveraging technology that performs accurately across demographic groups and classes, automated monitoring could potentially facilitate standardized oversight and monitoring, resulting in more consistent management practices, such as promotions or scrutiny, and may help foster equal treatment of employees.

ii. **Potential Challenges**

While this technology has potential to foster equal treatment of employees, we must also acknowledge that different groups may have divergent conclusions about how “fair” the outcomes of a particular model are, and it is essential to identify the risks and the impact of the outcomes generated by these technologies. There are also concerns about the potential for surveillance or monitoring to introduce
Bipartisan Policy Center
Where democracy gets to work

additional bias or discrimination in the workplace. These concerns and how data is utilized to ensure fairness and equal opportunities in the workplace should be carefully considered.

Another major concern regarding automated worker surveillance and management’s privacy. While individuals generally enjoy a reasonable expectation of privacy, sometimes protected by law, expectations of privacy at work are different. Additionally, cutting-edge technologies have the potential to expand workplace surveillance capabilities, thereby adding new layers and more complexity to longstanding debates about privacy in the workplace. Using AI technologies that process keystroke monitoring and/or web-browsing can enable employers to make data-driven predictions about employee productivity and on a much wider scale than ever before. If this data reveals information about workers’ protected health or disability status, the privacy risks are significant. Furthermore, collecting, analyzing, and storing this data can also create data protection challenges. As this example demonstrates, carefully considering the implications of enhanced surveillance capabilities in the workplace is important.

Issues around power asymmetries between employers and workers are also prompted by worker surveillance and management. Intrusive monitoring techniques can be perceived as intimidating, exacerbate existing power imbalances, and may lead to worker stress and dissatisfaction. Surveillance or monitoring may also lead to uninformed or incomplete information regarding a worker’s productivity. Employers should be especially careful when using this information to make employment or pay decisions. There may be tasks performed offline or those not easily traced, making it difficult to capture the extent of a worker’s performance. Additionally, employees may take deliberate steps to protect their privacy, affecting the extent to which employers can effectively monitor their work.

b. Policies, practices, or standards to protect workers (Question 5(a-c))

i. Guidelines, standards, or best practices

Developing guidelines, standards, or best practices can play a crucial role in shaping the design of automated worker surveillance and management systems, with a particular focus on protecting workers’ rights. It is critical the Federal government supports research on the prevalence and impact of these systems to understand the usage, effectiveness, and potential risks associated with these technologies in the workplace. This research should inform the development of guidelines and regulations that protect worker privacy and security while fostering innovation in the workplace.

Through our work developing recommendations for our AI National Strategy for Congress, the following recommendations are also applicable in this context. They include funding for research and development, transparency around data use practices, and building on existing guidelines, standards, or best practices when possible.

Policymakers should focus on allocating funding for research, development, and testing to support the exploration of technical and non-technical solutions that address ethical concerns in AI. From our AI and...
Ethics issue brief, we note “Congress should support funding for agencies interested in adopting programs (such as regulatory sandboxes) for temporarily approving, testing, and monitoring innovative AI tools in limited markets. Programs should have necessary safeguards and oversight processes.” Additionally, diversity among perspectives and researchers’ experiences is important to ensure comprehensive and equitable outcomes.

Transparency is crucial to building trust when using surveillance and management systems. Transparency into the ways in which workers’ data is collected and why can help inform workers of risks they might assume when the technology is employed. Another important aspect is providing workers transparency into the additional layers a business provides regarding privacy protection. This can help alleviate concerns around what information is being collected, used, and shared.

Reviewing existing guidelines, standards, and practices to determine if they encompass automated surveillance and management is key. It’s important to build off existing frameworks, when possible, address gaps, and tailor regulations to meet the needs of today’s workforce. We’ve provided a non-exhaustive list of various guidelines and frameworks that should be reviewed.

- The National Institute of Standards and Technology (NIST) released an [AI Risk Management Framework](https://www.nist.gov/) (2023), a [Privacy Framework](https://www.nist.gov/) (2020), and a [Cybersecurity Framework](https://www.nist.gov/) (2018). These frameworks are voluntary and designed to help organizations to manage their various risks, improve innovation, and protect individuals.
- The White House [Blueprint for an AI Bill of Rights](https://www.whitehouse.gov/) provides steps to integrate “principles for building and deploying automated systems that are aligned with democratic values and protect civil rights, civil liberties and privacy.”
- The Partnership on Employment & Accessible Technology, funded by the Office of Disability Employment Policy at the Department of Labor, produced an [AI & Disability Inclusion Toolkit](https://www.dol.gov/) and [The Equitable AI Playbook](https://www.pedac.org/) that teaches employers how AI tools function in the workplace and how to implement AI in ways that are equitable for employees with disabilities and foster workplace inclusion.
- ISO, an international standards setting organization released [ISO 45001](https://www.iso.org/), a standard to help organizations improve occupational health and safety management systems.
- Society for Human Resource Management published [resources](https://www.shrm.org/) on best practices for employers using workplace surveillance to ensure employee privacy and maintain ethical monitoring practices.

ii. Policy Approaches

Several existing laws already govern workplace monitoring. The [Electronic Communications Privacy Act of 1986](https://www.ecpa.org/) (ECPA) (18 U.S.C. Section 2511 et seq.) and common-law protections against invasion of
privacy govern the monitoring of digital and electronic communication. While these laws provide some safeguards, businesses may monitor employee activity if there are legitimate business reasons or with consent of monitoring. The National Labor Relations Act of 1935 (NLRA) (Section 7 & 8(a)(1)) prohibits employers from infringing on employees protected and concerted activities such as collective bargaining or mutual protection.

Some state laws set restrictions on employee monitoring and surveillance. For instance, a Connecticut law requires employers to provide notice to perform electronic monitoring of employees, while a New York law requires employers to provide written notice upon hiring and annually to employees that they may monitor or intercept electronic communications. Other laws, like the Illinois Biometric Information Privacy Act, impose limits on processing particular types of data in multiple contexts, including workplaces. Furthermore, several state constitutions, such as in California, Florida, Louisiana, and South Carolina, explicitly state that residents have a right to privacy, extending employees’ expectations of privacy.

Policymakers should review and consider building upon existing regulations where possible, considering the evolving technological landscape. By examining existing policies and regulations, policymakers can gain valuable insights and adopt a comprehensive approach that safeguards workers’ rights and employer needs. Moreover, it is important to consider how passing any regulations may indirectly influence strategies and negotiations around designing regulations for automated surveillance and management systems. It’s important to keep this in mind as policymakers work to pass comprehensive data privacy laws and AI-related laws in Congress and state legislatures.

ii. Policy Considerations

The extent of agencies’ authorities in addressing issues involving automated systems is often unclear. Enhancing policies or guidelines can provide clarity around agencies’ authority to ensure responsible development, deployment, and utilization of automated worker surveillance and management systems. This can include internal policies governing the agencies’ own use of workplace surveillance tech or external-facing guidance documents advising the private sector on workplace surveillance issues and best practices for risk mitigation.

For instance, the Federal Trade Commission (FTC) has the authority to protect against unfair or deceptive privacy- and security-related conduct. With the increasing concerns surrounding commercial surveillance and data security, the FTC announced an Advance Notice of Proposed Rulemaking. By examining the use of automated surveillance and management systems and reviewing the agency’s existing enforcement actions, the FTC can take appropriate steps to protect workers' privacy and security.

Federal agencies, such as the Equal Employment Opportunity Commission, should review their existing authority to govern the use of automated management and surveillance. Agencies should also consider
funding more research on automated workplace surveillance and management tools and their impact on workers. Further research on these systems will contribute to a better understanding and guide future governance frameworks.

Finally, considering the limitations of agencies’ current authority and capabilities, a comprehensive national consumer data privacy legislation is crucial to addressing the various challenges posed by automated worker surveillance and management. Effective privacy regulations are essential to ensuring automated systems are developed and deployed in a way that ensures protection of individuals’ personal information.

III. Closing

Policymakers must carefully consider ways to address concerns of vulnerable populations, foster a competitive workforce, protect workers’ rights and privacy, and promote ethical and responsible practices concerning automated worker surveillance and management systems. We would like to express our gratitude to OSTP for commencing this important first step toward preparing our workforce for the future. We appreciate the opportunity to share our considerations and insights on automated surveillance and management in the workplace. We remain committed to serving as a resource moving forward, collaborating with stakeholders, and contributing to the ongoing dialogue surrounding the responsible and equitable integration of technology in the workplace.

Sincerely,

Bipartisan Policy Center Technology Project
We from the Center for AI & Digital Policy (CAIDP) attach our statement in response to the Request for Information - Automated Worker Surveillance and Management (OSTP-TECH-2023-0004-0001) issued by the OSTP.

In summary, we recommend:

1. The OSTP AI Bill of Rights be implemented, most pertinently the Data Privacy section protecting workers from surveillance along with the Algorithmic Discrimination Protections.

2. Enactment of federal legislation for AI governance based on the Universal Guidelines for AI including the Right to Transparency, Identification Obligation, Fairness Obligation, Assessment and Accountability Obligation, Accuracy, Reliability, and Validity Obligations, and Prohibition on Secret Profiling.

3. The OECD AI Principles, which the U.S. has already endorsed, should be implemented, specifically, Human Centered Values and Fairness Principles, Robustness, Security, and Safety, and Accountability.

4. The OSTP issues a statement in support of the Council of Europe AI Treaty, which would be a globally binding treaty on AI.

We support the OSTP effort to address immediate and critical harms caused by unchecked deployment of AI-systems in the workplace. We would welcome the opportunity to speak with you further about these recommendations.

Attachments

CAIDP_OSTP_RFI_15062023
CAIDP welcomes the opportunity to provide comments on the OSTP’s RFI\(^1\) on worker rights with respect to automated systems used to monitor, manage, and evaluate workers. In this statement we provide general recommendations relating to items covered under Questions No. 4 (data and research related questions) and No. 5 (policies, practices, or standards that could protect workers). We specifically recommend that OSTP:

1) Pursue implementation of the AI Bill of Rights, which states that individuals should be free from unchecked surveillance.

2) Support the adoption of the Universal Guidelines for AI, which allocates rights and responsibilities in the use and deployment of AI systems

3) Support implementation of the OECD AI Principles, which includes principles for Human-Centered Values and Fairness; Robustness, Security, and Safety; and Accountability.

4) Support adoption of a comprehensive treaty for AI at the Council of Europe that covers both public and private AI systems

About CAIDP

The Center for AI and Digital Policy (CAIDP) is a non-profit, global research and education organization based in Washington, D.C. Our mission is “to promote a better society, more fair, more just — a world where technology promotes broad social inclusion based on fundamental rights, democratic institutions, and the rule of law.”\(^2\) We publish annually the Artificial Intelligence Office of Science and Technology Policy, Request for Information; Automated Worker Surveillance and Management, [3270-F1], https://www.whitehouse.gov/wp-content/uploads/2023/05/050123_OSTP_RFI_PREPUBLISH.pdf

\(^1\) Office of Science and Technology Policy, Request for Information; Automated Worker Surveillance and Management, [3270-F1], https://www.whitehouse.gov/wp-content/uploads/2023/05/050123_OSTP_RFI_PREPUBLISH.pdf

\(^2\) CAIDP, https://www.caidp.org
and Democratic Values Index (AIDV), a comprehensive overview of AI policies across the world. In our 2023 edition, we note the U.S. expressed commitment to democratically-aligned AI through the endorsement of the OECD/G20 AI Principles and encouragement of public participation. However, the lack of a legal framework implementing AI safeguards raises concerns on the U.S.’s capability to monitor AI practices effectively.

We support the OSTP the Blueprint for the AI Bill of Rights. We also support the previous Executive Order 14091 (Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government), in which the Administration commits to investigating whether automated surveillance and management systems “contribute to unjustified different treatment or impacts,” and the Executive Order 14025 (Worker Organizing and Empowerment).

Worker Management with AI

Worker management with AI-based tools increases occupational hazards, risks to physical and mental safety, automates invasive, oppressive and unfair labor practices in the following ways:

1. *Increasing risk of injury and reduction in occupational safety of workers*: The relentless implementation of AI in workforce management is leading to several significant adverse consequences. For example, Amazon’s handheld scanners track the productivity of warehouse workers on a metric of how many items are loaded onto trucks and how many people are working on that shift. These scanners pressure workers into moving more items with fewer people. Workers and regulators both have said that Amazon’s use of high-tech monitoring has led to immense pressure on workers, resulting in serious injury rates nearly double those at other companies’ warehouses.

---

4 Id. at pg. 1085
5 CAIDP, *Support the OSTP AI Bill of Rights*, [https://www.caidp.org/statements/ostp/](https://www.caidp.org/statements/ostp/) (October 4, 2022)
2. Automation of coercive and unfair labor practices at the workplace: AI monitoring also enables a level of monitoring that infringes on workers’ rights to privacy, expression, and assembly. For example, Amazon’s surveillance technology stifles workers from unionization efforts, such as by placing cameras by mailboxes during union voting periods.\(^\text{10}\) This can be seen as an effort to intimidate or discourage workers as well as create a climate of fear and repression in the workplace. These concerns go beyond the bias and discrimination concerns that Executive Orders 14091\(^\text{11}\) and 14025\(^\text{12}\) have addressed.

3. Automation of exploitation and unfair labor standards: Amazon uses delivery service providers (DSPs) as contractors, meaning they do not provide workers’ compensation, insurance, guaranteed minimum wage or overtime compensation.\(^\text{13}\) The algorithms, apps, and devices underlying Amazon’s logistics and delivery operations result in exploitative and unfair labor standards by “tracking every move including backup monitoring, speed, braking, acceleration, cornering, seatbelt usage, phone calls, texting, in-van cameras that use artificial intelligence to detect for yawning, and more".\(^\text{14}\) Because of how these systems function and the opaque decision-making processes it is difficult to contest or challenge these decisions or understand the logic behind a particular outcome of decision. These algorithmic practices are now the subject of litigation Nevada\(^\text{15}\) in a case where an Amazon delivery driver’s car crashed into another car causing life-changing spinal cord and brain injuries to Ans Rana, a 24-year-old man. The substance of the allegation against Amazon centers on the algorithmic models underlying it’s logistics operations and intense tracking of delivery drivers that place “unrealistic and dangerous speed expectations” which have caused similar crashes by overworked delivery drivers.

DSPs are subject to dynamic pricing based on demand and routes, with quantitative digital evaluations of their “on-the-job behavior” determining bonuses. This practice allows firms to differentiate wages for workers without transparency behind their decisions. At companies such as Uber, this dynamic pricing system implicitly manipulates individual worker’s behavior. Professor Dubal classifies this as algorithmic wage discrimination, which is “a practice in which

\(^{10}\) Washington Post, Amazon monitors its warehouse staff, leading to unionization efforts, https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions/ (December 2, 2021)


\(^{15}\) Ans Rana v. Amazon Logistics, Eighth Judicial District Court, Clark County, Nevada, Docket No: A-21-843217-C
individual workers are paid different hourly wages—calculated with ever-changing formulas using granular data on location, individual behavior, demand, supply, and other factors—for broadly similar work." She argues it is a “deeply predatory and extractive labor practice” that preys on vulnerable workers while maintaining economic instability.\textsuperscript{16} Such opaque systems hamper the due process and ability of workers to contest the decisions.

\textit{Worker Surveillance with AI}

AI based tools enable workplace surveillance in an unprecedented manner. It has been reported that eight out of the ten largest employers in the United States employ measures to track individual worker productivity metrics, often in real time.\textsuperscript{17} The depth, breadth and comprehensive reach of continuous monitoring practices enabled by AI clearly violate workers' rights to privacy and can have severe implications on their access to opportunities, autonomy, and dignity. Moreover, surveillance practices normalized in work context reinforces a culture of normalization of such practices and infringements upon privacy and freedom of speech and assembly in other contexts – such as social media or public spaces.

1. \textit{Unfair performance evaluation through AI-enabled surveillance}: One notable example of such surveillance is witnessed in Walmart. The corporation has secured a patent for a system that permits monitoring of both workers and customers through auditory signals.\textsuperscript{18} This system can evaluate employee "performance metrics" by capturing sounds such as the rustling of bags and scanner beeps at the checkout line. It can then estimate the number of items in bags and the total bag count. Further, it can detect conversations of customers in line and verify if employees are providing customer greetings. While Walmart asserts that this innovation is designed to ensure job performance efficiency and accuracy, it has sparked serious debates on privacy and fairness. This arises from concerns about the system's potential lack of comprehension of nuances and aberrations of human behavior, which may lead to an excessively invasive surveillance approach.

2. \textit{Discrimination through AI-enabled surveillance}: AI-based surveillance and management systems are also known for additional bias and adverse impacts on workers with disabilities. Since these systems are designed with typical or productivity and behavioral expectations, the atypical way of completing tasks or the speed of completion can negatively flag workers with disabilities,\textsuperscript{19} or even disclose the disabilities of workers to employers where

\begin{thebibliography}{99}
\bibitem{16}Dubal, On Algorithmic Wage Discrimination
\end{thebibliography}
previously not disclosed. Even if such knowledge of disability is not used in a future employment decision, the employers could still be alleged to have discriminated against the worker due to a perceived disability.\textsuperscript{20}

Furthermore, despite what companies may believe, evidence has shown that monitoring employees does not necessarily equate to increased productivity or improvements in workplace culture.\textsuperscript{21} On the contrary, it has been suggested that this practice can damage the latter and spur counterproductive behavior.\textsuperscript{22} In fact, many tech employees have expressed a strong disapproval of such surveillance measures, stating they would rather quit their job than be continuously monitored during work hours.\textsuperscript{23}

**Existing Responses and Frameworks**

The emerging trend of invasive and exploitative surveillance technologies in workplaces has not gone unnoticed.

In response to the escalating use of invasive "bossware" that tracks remote employees' activities, the US National Labor Relations Board is planning intervention measures to protect workers' rights.\textsuperscript{24} The government body aims to prevent such intrusive surveillance from infringing on employees' rights to unionize and is advocating for obligatory employer disclosure on the extent of their monitoring practices.\textsuperscript{25} However, in the cases where workers are not notified of surveillance practices and the employer is not disclosing the practice to NLRB, such practices continue under the radar. In 2021, the FTC warned businesses about potential unfair or deceptive practices, including the use or sale of biased algorithms.\textsuperscript{26} This guidance urges businesses to take responsibility for their AI practices and uphold standards of truthfulness, fairness, and equity. For both NLRB and FTC protections to be meaningful, there must be mandates in place for

\textsuperscript{20} Sonderling, K.E., Kelley, B.J., Casimir, L.: The promise and the peril: artificial intelligence and employment discrimination. Univ. Miami Law Rev. 77, 1–87 (2022)
employers to disclose the use of these monitoring and management systems to workers and unions as well.

U.S. Senator Bob Casey (D-PA) recently sent a letter to Department of Labor Secretary Marty Walsh, urging the Department to track surveillance technologies used in workplaces.27

The Office of Science and Technology Policy (OSTP) has taken a prominent stance in defining and addressing issues related to surveillance technology through its Blueprint for an AI Bill of Rights. The Blueprint expressly defines surveillance as the use of products or services that have the potential to detect, monitor, intercept, collect, exploit, preserve, protect, transmit, and/or retain data, identifying information, or communications concerning individuals or groups. This extends to both government and commercial uses of surveillance technologies, specifically when coupled with real-time or subsequent automated analysis, and when such systems have the potential to significantly impact individuals’ or communities’ rights, opportunities, or access.

The OSTP’s AI Bill of Rights categorically asserts that continuous surveillance and monitoring should not be employed in contexts such as education, work, and housing where its use could potentially limit rights, opportunities, or access.28 It further advocates for transparency by stating that individuals should, whenever possible, have access to reports confirming that their data decisions have been respected and providing an assessment of the potential impact of surveillance technologies on their rights, opportunities, or access.

This clear directive from the OSTP is bolstered by other domestic and international bodies championing similar principles. The UNESCO AI Recommendation, adopted by all 193 member states, explicitly prohibits the use of social scoring and mass surveillance due to their infringement on human rights.29 Likewise, the U.S. has endorsed the OECD AI Principles, which underscore Human-Centered Values and Fairness, mandating that AI actors respect freedom, dignity, autonomy, and internationally recognized labor rights.30

Workers have already begun leveraging existing regulations such as the GDPR and the California Privacy Protection Act to demand transparency in the wage algorithms and data

28 OSTP, Blueprint for an AI Bill of Rights
29 UNESCO, UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence, https://www.unesco.org/en/articles/unesco-member-states-adopt-first-ever-global-agreement-ethics-artificial-intelligence?TSPD_101_R0=080713870fab200073e3c41b5fcef8ea2697d2ae4ba78f92585160eaa92c366e1a4fa632ab5ea3a08ceb88a91430098d0475f1e6b230a4d6e8d2ad0df5b0b326832df24f2b4faea0f339a0322c98ead4662e58b09859a188390167353665#:~:text=Banning%20social%20scoring%20and%20mass,used%20in%20a%20broad%20way (April 20, 2023)
30 OECD, Human-centered values and fairness (Principle 1.2), https://oecd.ai/en/dashboards/ai-principles/P6
extracted from their labor. They have also used business association laws to maximize worker controls through “parallel data collection, collective data ownership, and sale of ownerships.”

CAIDP President, Merve Hickok emphasizes the importance of worker unions in upholding workers’ rights through 1) demanding contractual protections in union contracts, and 2) providing relevant information on worker surveillance to the FTC and NLRB to support investigation and enforcement activities. She stresses the need for worker representation in the design and governance of mutually beneficial algorithmic systems. Professor Dubal recognizes the merit in these cooperative efforts but also proposes a direct “statutory or non-regulatory ban” on algorithmic wage discrimination including digitized piece pay to reduce incentive on data extraction and retention.

CAIDP has promoted better labor protections in workplaces and hiring practices subject to AI decision-making. We previously advised the EEOC to consider the impact of algorithmic systems in the workplace as a top priority for the Fiscal Years 2023-2027. We recommended that the EE ensure that “abilities truly necessary for the job” are measured along with the creation of “internal capacity to responsibly understand the benefits, risks and limitations of algorithmic systems.”

Marc Rotenberg, Executive Director of CAIDP, has also called for worker participation in the development of relevant technology to safeguard personal information of employees and preserve human judgment. In addition, Merve Hickok has previously highlighted the power imbalances between workers and employers. To resolve these impacts, Hickok recommends, first and foremost, legislation safeguarding workers’ rights against being subject to surveillance and exploitative technological practices. Hickok notes “claims and embedded design decisions include fundamentally erroneous assumptions, such as the ability for technology to correctly capture a human’s complex nature, or infer emotions and sentiments, or that human behavior can always be predicted.”

CAIDP has recommended that pseudoscientific “biometric categorization” and “emotion analysis” systems are banned. These systems often require the collection and processing of highly personal and sensitive data, such as facial features or emotional state, which raises privacy concerns.

---

31 Dubal, On Algorithmic Wage Discrimination.
32 Id.
34 Id.
35 Dubal, On Algoritmic Wage Discrimination
37 https://web.mit.edu/gtmarx/www/labor_hr_testimony.pdf
38 Hickok and Maslej, A policy primer and roadmap on AI worker surveillance and productivity scoring tools
concerns. This level of invasiveness and control leads to infringement of people’s dignity and agency.

**Our Recommendations**

The Center for AI and Digital Policy (CAIDP) recommends that:

1. The OSTP AI Bill of Rights be implemented, most pertinently the Data Privacy section protecting workers from surveillance along with the Algorithmic Discrimination Protections.

2. Enactment of federal legislation for AI governance based on the Universal Guidelines for AI including but not limited to:

   a. **Right to Transparency:** All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.
   
   b. **Identification Obligation:** The institution responsible for an AI system must be made known to the public.
   
   c. **Fairness Obligation:** Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.
   
   d. **Assessment and Accountability Obligation:** Assessment and Accountability Obligation. An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.
   
   e. **Accuracy, Reliability, and Validity Obligations:** Institutions must ensure the accuracy, reliability, and validity of decisions.
   
   f. **Prohibition on Secret Profiling:** No institution shall establish or maintain a secret profiling system.

3. The OECD AI Principles, which the U.S. has already endorsed, should be implemented including but not limited to:

   a. **Human-Centered Values and Fairness Principle:** AI actors must respect freedom, dignity and autonomy, [...] and internationally recognized labor rights.
   
   b. **Robustness, Security, and Safety:** AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.
c. Accountability: Organizations and individuals developing, deploying, or operating AI systems should be held accountable for their proper functioning in line with the OECD’s values-based principles for AI.

4. The OSTP issues a statement in support of the Council of Europe AI Treaty, which would be a globally binding treaty on AI.

We applaud OSTP on this initiative towards to ensure that AI systems do not undermine workers’ rights, opportunities, access, health or safety. Thank you for your consideration of our views. We would welcome the opportunity to speak with you further about these recommendations.

Marc Rotenberg  
CAIDP Executive Director

Merve Hickok  
CAIDP President

Lorraine Kisselburgh  
CAIDP Chair

Wonki Min  
CAIDP Board Member

Lyantoniette Chua  
CAIDP Teaching Fellow

Nidhi Sinha  
CAIDP Research Fellow

Christabel Randolph  
CAIDP Law Fellow

Sunny Gandhi  
CAIDP Research Assistant
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0160
Comment on FR Doc # 2023-09353

Submitter Information

Email: [redacted]

General Comment

Comments submitted on behalf of the Owner Operator Independent Drivers Association

Attachments

OSTP 2023-09353 - Automated Surveillance
June 15, 2023

Mr. Alan Mislov
Assistant Director for Data and Democracy
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW
Washington, D.C. 20504

Re: FR Docket # 2023-09353, “Automated Worker Surveillance and Management (Request for Information)”

Dear Mr. Mislov:

The Owner-Operator Independent Drivers Association (OOIDA) is the largest trade association representing the views of small-business truckers and professional truck drivers. OOIDA has more than 150,000 members located in all fifty states that collectively own and operate more than 240,000 individual heavy-duty trucks. OOIDA’s mission is to promote and protect the interests of its members on any issues that might impact their economic well-being, working conditions, and the safe operation of commercial motor vehicles (CMVs) on our nation’s highways.

The federal government mandates a system of automated surveillance for America’s truckers that puts more stress and pressure on drivers and has failed to yield any improvements to safety or compensation. In 2012, Congress passed, and President Obama signed into law, the Moving Ahead for Progress in the 21st Century Act (MAP-21) (P.L. 112-141), which required motor carriers to install and use an electronic logging device (ELD) in trucks to monitor their drivers. These devices are hardwired to a truck’s engine and automatically record information about the truck and its operation at all times. By law, this information must include: date; time; location information; engine hours; vehicle miles; and identification information for the driver, authenticated user, vehicle, and motor carrier. ELD manufacturers are permitted to self-certify their devices, and MAP-21 contained no restrictions on what information could be collected by private industry or how they could use the information.

This automated surveillance has yielded no benefits for truckers or the public. While ELDs have improved compliance with some federal regulations, safety outcomes have worsened. Since the

ELD mandate took effect in 2017, the total number of fatalities in large truck crashes has slowly, but steadily increased, even when adjusting for the number of miles travelled.\(^2\) Similarly, with the exception of 2020 and pandemic-related effects, the number of injuries and crashes involving large trucks has also steadily increased.\(^3,4\)

While having no safety benefits, the mandate has simultaneously failed to improve pay for truckers. When adjusted for inflation, average annual wages for heavy and tractor-trailer truck drivers remained about the same in 2022 as it was from 2016 to 2019, the years immediately before and after the ELD mandate was implemented.

Aside from having no safety or wage benefits, this automated surveillance puts even greater stress on drivers. Drivers’ movements can now be monitored down to the second to allow scrutiny and second-guessing under the guise of compliance with federal regulations. As a direct result, they feel enormous pressure when trying to find permissible parking to take a federally mandated rest break or complete their job under the threat of discipline from their employer.

OOIDA appreciates that the OSTP is examining the potentially harmful effects of automated surveillance on workers, but truckers have reason to doubt that the federal government and the Biden Administration are really listening to them about these concerns. Currently, there are two open rulemaking processes within the U.S. Department of Transportation that would expand the mandatory surveillance of truck drivers.

The Federal Motor Carrier Safety Administration (FMCSA) has initiated a rulemaking to revise ELD regulations (FMCSA-2022-0078) to both expand the type of data that ELDs would be required to record and require data to be recorded at more frequent intervals. This would allow employers to collect even greater information about their employees under the illusion of a government mandate.

FMCSA has also initiated a rulemaking (FMCSA-2022-0062) that could require all trucks to be “equipped with electronic identification (ID) technology capable of wirelessly communicating a unique ID number when queried by a Federal or State motor carrier safety enforcement personnel.” FMCSA is considering requiring these transmitters to provide law enforcement with information about the driver, including information about their hours of service and medical certification. In other words, the federal government wants to mandate trackers on truckers so that they can be remotely monitored at any moment by law enforcement. Due to the absence of any research demonstrating how this technology would improve safety, the motivation for pursuing this rulemaking appears to be nothing more than adding convenience for enforcement agencies. This creates concerns about the potential for unreasonable search and seizure and violation of drivers’ privacy rights under the 4th Amendment to the U.S. Constitution.

---


\(^3\) Ibid., p. 13

\(^4\) Ibid., p. 18

The current ELD mandate, as well as these two proposed rulemakings, are harmful because they would significantly expand both government and industry tracking of workers. There are few, if any, other professions where federal, state, and local government have the right and ability to see what a worker is doing at any given minute. But even worse, these types of policies are a “foot in the door” for employers to use expansive tracking technology. With the government requiring an ELD in every truck, and no limits on what else the ELD can record or how businesses can use the information, employers can use the devices to monitor almost everything about a driver. Outside of work functions, drivers may also use their truck for personal reasons under “personal conveyance.” If an employer continues to collect data, such as location, while a driver is off-duty, this could be used to learn about potentially protected information such as an individual’s political or religious affiliation depending on when and where they park their truck.

Cornell University Associate Professor Dr. Karen Levy examines the scope of this data collection and how it is used in her book Data Driven: Truckers, Technology, and The New Workplace Surveillance. She describes the detailed information that ELDs are used to collect, including “a driver’s fuel efficiency and idling time, speed, geolocation and geofencing…lane departures and braking/acceleration patterns…tire inflation, and vehicle maintenance and diagnostic information.” This wealth of data has enabled carriers to evaluate truckers’ behavior in real-time and potentially second-guess a driver’s decisions.

Beyond this, ELD data can be used by carriers to measure an individual driver’s performance, compare it to colleagues, and in turn, incentivize or “shame” drivers. While these types of programs may offer drivers beneficial rewards in some instances, professional drivers operate under enormous stress and face many obstacles outside of their control. They experience delays due to weather, crashes, or detention time, or waste time looking for acceptable parking on a daily basis. With so many factors outside of a driver’s control, OOIDA believes it is extremely difficult for granular ELD data to capture the complete picture of their daily, weekly, and monthly experience and performance. Additionally, carriers can misinterpret or abuse this data to put pressure on drivers that both compromises their safety and ignores the challenges they face.

Thank you for your consideration of these comments and suggestions. We hope that OSTP will use this feedback, and the feedback from other commenters, to inform the ongoing rulemakings at FMCSA and protect truckers from further government and employer surveillance.

Sincerely,

Todd Spencer
President & CEO
Owner-Operator Independent Drivers Association, Inc.

---

7 Ibid., p. 67.
8 Ibid., p. 70.
The Association for Computing Machinery (ACM) is the longest established and with more than 50,000 American members – the largest association of individual professionals engaged in all aspects of computing in the nation. A non-lobbying and otherwise wholly apolitical organization, ACM’s mission includes providing unbiased, expert technical advice to policymakers on matters of our members’ wide-ranging expertise. That work is accomplished in the United States by and through ACM’s U.S. Technology Policy Committee (USTPC).

In December of 2022, USTPC released the attached Statement on Principles for the Development and Deployment of Equitable, Private, and Secure Remote Proctoring Systems noting that, as such systems become a pervasive component of online education, institutions and "technology vendors at a minimum must address major issues of equity, privacy, security, accessibility, and efficacy." We also expressly observed that the use of such systems in an educational context had the potential to "embolden the implementation of other surveillance systems," including specifically employee monitoring software.

USTPC believes that many of the guiding principles set forth in its December 2022 Statement are germane to OSTP's present inquiry and is pleased to submit them for the Office's consideration and potential application in this critical context.

**Attachments**

ACM_USTPC_OSTP Remote Worker Surveillance Comments 061523
June 15, 2023

Submitted Electronically

Hon. Arati Prabhakar, Ph.D., Director
Office of Science and Technology Policy
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Re: Request for Information Concerning Automated Worker Surveillance and Management, Document No. 2023-09353

Dear Dr. Prabhakar:

The Association for Computing Machinery (ACM) is the longest established and – with more than 50,000 American members – the largest association of individual professionals engaged in all aspects of computing in the nation. A non-lobbying and otherwise wholly apolitical organization, ACM’s mission includes providing unbiased, expert technical advice to policymakers on matters of our members’ wide-ranging expertise. That work is accomplished in the United States by and through ACM’s U.S. Technology Policy Committee (USTPC).

In December of 2022, USTPC released the attached Statement on Principles for the Development and Deployment of Equitable, Private, and Secure Remote Proctoring Systems noting that, as such systems become a pervasive component of online education, institutions and "technology vendors at a minimum must address major issues of equity, privacy, security, accessibility, and efficacy." We also expressly observed that the use of such systems in an educational context had the potential to "embolden the implementation of other surveillance systems," including specifically employee monitoring software.

USTPC believes that many of the guiding principles set forth in its December 2022 Statement are germane to OSTP's present inquiry and is pleased to submit them for the Office's consideration and potential application in this critical context.

ACM U.S. Technology Policy Committee
www.acm.org/public-policy/ustpc

342
Thank you for your consideration of the attached Statement.

cc: Alan Mislove, Assistant Director for Data and Democracy

Attachment:

(b) (6)

Alec Yasinsac
USTPC Vice Chair
STATEMENT ON PRINCIPLES FOR THE DEVELOPMENT AND DEPLOYMENT OF EQUITABLE, PRIVATE, AND SECURE REMOTE PROCTORING SYSTEMS

The ACM US Technology Policy Committee (USTPC)\(^1\) notes that many universities, schools, and professional certification organizations have employed remote proctoring (RP) systems during the COVID-19 pandemic. Such systems are intended to permit enrolled students and other individuals taking tests (including standardized or certification examinations) to complete them by computer in their homes or other noninstitutional settings. RP systems vary in their designs and capabilities, but virtually all use software as digital exam proctors. Nearly all RP systems deploy as integrated packages that include both test-administration and -monitoring software (i.e., the software both administers tests and monitors test-takers).\(^2\)

Designers and providers of commercial RP systems represent that they deliver the same level of test security as achieved when tests are administered “live” in classrooms or testing centers and are proctored in person. The use of RP technology is controversial, however, among some academics

---

\(^1\) The Association for Computing Machinery (ACM), with more than 100,000 members worldwide, is the world’s largest educational and scientific computing society. ACM’s US Technology Policy Committee (USTPC), currently comprising more than 175 members, serves as the focal point for ACM’s interaction with all branches of the U.S. government, the computing community, and the public on policy matters related to information technology. This statement’s principal author for USTPC is Christopher Kang. Primary additional contributors include Committee Chair Jeremy Epstein and Committee members Cory Doctorow, Simson Garfinkel, and Jeanna Matthews.

\(^2\) The test-giving portion presents test questions, records student answers, ensures the security of the test instrument, and attempts to isolate the test computer. The test-monitoring portion attempts to ensure that the test-taker is not cheating. Some systems simply record student interactions, while others monitor the student computer’s screen or activate the student’s webcam or microphone. Many systems also augment monitoring with artificial intelligence and machine-learning algorithms designed to flag suspicious behavior for review. For example, some systems use gaze-tracking software to monitor the movement of the student’s eyes in an attempt to determine where the student is looking, which might indicate that they are using a second computer, a cell phone, or some other forbidden testing aid.
and institutions\(^3\) who question its reliability, accuracy, and racial “impartiality.”\(^4\) They specifically note its potential for serious adverse, sometimes egregious,\(^5\) effects on users’ privacy.\(^6\)

Others have observed that because RP systems are not cost-free to acquire and deploy, educational administrators must decide whether individual test-takers must pay—and, if so, how much—to take an RP-facilitated exam.\(^7\) Whenever such costs are assessed to individuals, the financial inability of some to pay the fees raises critical questions that administrators must address as a matter of equity, fairness, and potentially antidiscrimination law.

---


\(^6\) Universities and other organizations employing RP must comply with a range of federal statutes, including the Family Educational Rights and Privacy Act (FERPA), Individuals with Disabilities Education Act (IDEA), guidance provided directly by the Department of Education, and Section 508 of the Rehabilitation Act of 1973 when the software is used by a U.S. government entity. This creates a complex legal and regulatory environment that administrators must navigate. Administrators must decide not just which RP platforms to use but also which features to enable and how to respond to the concerns of students and faculty. See Andy Dua. “Using Human Intervention and Technology to Secure Test-Taking,” Forbes, May 4, 2021, www.forbes.com/sites(forbesbusinesscouncil/2021/05/04/using-human-intervention-and-technology-to-secure-test-taking


\(^7\) The pricing structure for RP systems is often also opaque. Costs range from an estimated $4 per hour per test to $15 per hour per test, and more for platforms that require more complex monitoring. See, e.g., Jean Dimeo. “Online Exam Proctoring Catches Cheaters, Raises Concerns,” Inside Higher Ed, May 10, 2017, www.insidehighered.com/digital-learning/article/2017/05/10/online-exam-proctoring-catches-cheaters-raises-concerns
Such issues also arise whenever RP systems and associated institutional policies for their use require test-takers to have access to a computer, Wi-Fi, and/or broadband internet service, and/or to be alone in a room for the duration of an exam. It frequently is not possible, for example, for homeless and otherwise economically disadvantaged students and test-takers to satisfy these requirements. These issues notwithstanding, the use of RP technology is forecast to expand because of both the increased flexibility and perceived cost savings it offers educational and other test-administering institutions.

In the committee’s view, as RP technologies emerge as a pervasive component of online education, institutions and technology vendors at a minimum must address major issues of equity, privacy, security, accessibility, and efficacy. To that end, USTPC offers these guiding principles:

**EQUITY**

- Remote proctoring systems must be fair to all test-takers. A common feature of RP tools is that they provide some form of virtual inspection of the student’s environment during test-taking. This can produce inequitable outcomes to the disproportionate detriment of already marginalized learners, including:
  - **Homeless test-takers.** These students may have no choice but to take tests in cafés or parking lots within range of libraries or other public Wi-Fi hot spots. RP technologies typically deem these environments unacceptable, often without the possibility of appeal.

---

8 USTPC believes that policies regarding the use of RP should be effective, understandable to test-takers, and privacy-conscious in keeping with ACM’s [Code of Ethics and Professional Conduct](https://www.acm.org/codes), which counsels computing professionals to avoid harm, be cognizant of the public good, and thoroughly evaluate the impacts and risks of computing systems before deploying them. While written for ACM members and other computing professionals, these core precepts of the code also may be employed by policy makers assessing how to effectively regulate development and use of RP technologies.


10 Institutions also may be motivated to permanently adopt online or hybrid online/in-person learning strategies to expand their enrollments and their appeal to previously underrepresented and nontraditional students.

11 The issues addressed by these principles are not comprehensive. Others, including nontechnical considerations, should also concern policymakers. These include, for example, resolving whether parents must consent to the vendor-dictated terms of service for their minor child’s use of RP software, and what standards of disclosure and layperson comprehensibility will influence or dictate the content of such terms of service.

12 While beyond the scope of this statement, the committee also notes that the application of RP technologies may simultaneously embolden the implementation of other surveillance systems (e.g., employee monitoring software). See Jodi Kantor and Arya Sundaram. “The Rise of the Worker Productivity Score,” *New York Times*, August 14, 2022, www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html

13 The committee’s analysis and recommendations pertain to automated monitoring systems while recognizing that they may also well be relevant to systems that at least partially rely on human monitoring. The latter are likely to be designed and deployed much less frequently because they are costly and difficult to operate successfully at scale.
o Test-takers in broadband deserts. Some housed students have inadequate or no access to sufficiently robust broadband internet service to meet baseline RP requirements or to fully enable such systems. They, too, must take their exams in environments that RP tools reject. Previous work has found that access to broadband is strongly correlated with a person’s race and economic status.\textsuperscript{14}

o Test-takers in crowded homes. Many test-takers live in quarters where every room is necessarily occupied by at least one other person, often a person who cannot reasonably be expected to move, such as a parent working the night shift whose sleep cannot be interrupted during a remote exam. Not only can such students face immediate disqualification for failing to isolate themselves, but the very act of requiring them to show their environment to instructors or remote proctors is an invasion of both their privacy and the privacy of others with whom they share living space.

- Any deployed RP system, and the policies that govern its use, must accommodate these and similar cases without prejudice to the test-taker.

- RP technologies may have system requirements that exceed those of some students’ equipment, which often is configured only as minimally needed for students to play video games or participate in online discussion.\textsuperscript{15} Such requirements for hardware and high-performance internet connectivity may preclude some students from utilizing these systems.\textsuperscript{16} RP vendors and institutions thus must ensure that system requirements are comparable to prior course requirements without imposing onerous technical burdens on students. Institutions considering the use of RP technologies should also ensure that, when operating in resource-constrained environments (such as on older laptops or computers with less-than-optimal memory), users’ experience of the software’s operation will not be distracting to them or functionally degraded in material ways.\textsuperscript{17}

- Institutions should ensure that all students, regardless of their ability to pay associated fees, have full access to institutionally mandated RP systems.\textsuperscript{18}


\textsuperscript{15} For example, many systems simultaneously transmit two video streams—the video camera and the desktop—as well as run image-processing software on the test-taker’s system.

\textsuperscript{16} More broadly, testing systems may be incompatible or unstable on certain devices for a variety of reasons. For example, they may not be designed to work with newer processors. Emma Roth. “Intel’s 12th Gen CPU Can’t Handle the Bar Exam,” \textit{The Verge}, July 13, 2022, www.theverge.com/2022/7/13/23209784/intel-law-students-12th-gen-processor-bar-exam-examplefly-examssoft

\textsuperscript{17} Prior to enrolling in a class, the requirements needed to use RP systems should be made clear and students should be provided with a means of verifying without cost that they can successfully use any required RP system.

\textsuperscript{18} The committee notes that such accommodations are routinely made by institutions, such as when laboratory fees are waived based on financial hardship and sees no rationale for treating required software differently.
PRIVACY

- Data collection by RP technologies should be targeted, transparent, and minimized. Collected data should be retained for at most one year following the conclusion of the student's tenure at the educational institution.\(^{19}\)

- Test-takers using RP technologies must, at minimum,\(^ {20}\) be provided notices describing:
  - What data will be collected and how long it will be retained
  - Who will have access to data (e.g., administrators, automated systems, or teaching assistants)
  - How information collected may be used in determining academic misconduct

- Test responses should be segregated from non-test response data. Non-test response data includes audio and visual recordings of the test-taker, and technical information (e.g., the test-taker’s IP address and keystroke timing data). Access to these kinds of data should be independently controlled and logged.

- Data collected by RP technologies, especially sensitive data such as video and audio recordings, should be destroyed when they are no longer required by administrators. RP vendors should never retain data for any purpose, even if the material is anonymized or students are given the ability to “opt out” of such data retention.

- RP technologies should incorporate end-to-end encryption for all test-taking data,\(^ {21}\) both in transit and at rest.

- RP technologies should not access the local data on the test-taker’s computer. For example, the technologies should not scan the test-taker’s files in an attempt to locate unauthorized copies of testing materials.\(^ {22}\) Likewise, RP technologies should not include remote control features, such as the ability to move the test-taker’s mouse, select other windows, or enter keystrokes on the test-taker’s computer.\(^ {23}\)

\(^{19}\) A substantially shorter period may well be more appropriate, particularly when improper test-taker activity is not reasonably suspected or is determined not to have occurred.

\(^{20}\) Whenever technically feasible, as it ought to be in most cases, the committee also strongly recommends that RP system designers engineer systems to provide test-takers with visual previews of how the RP software will perceive their environments that flag items the software could or would consider violative of the exam’s protocols so that they may be redressed before the start of the remotely proctored test. Such features must be made fully compatible with audio description programs relied upon by visually impaired students.

\(^{21}\) Test-taking data includes responses, data collected as a result of monitoring, and test-taking metadata (such as IP addresses, mouse movements, and keystroke intervals).

\(^{22}\) See Note 5.

\(^{23}\) Although vendors may find it tempting to build remote control “help desk” functions into their products, the potential for abuse is too great; many other safer modalities are available for test-takers who require such support.
• RP technologies must be designed to automatically disable all tracking functions once exams for which they are employed have been completed. Such software also should provide test-takers with a transparent mechanism to easily and totally disable installed RP software as well as to wholly remove it from the test-taker’s computer.

• Data collected by RP technologies, including but not limited to screenshots and video/audio recordings, should be considered educational records under the Family Educational Rights and Privacy Act (FERPA), and institutions should be prepared to promptly share all information collected by RP technologies with students, as required by law, upon a student’s request.

• While FERPA provides a process for resolving student privacy violations, this process applies only to students and parents. Therefore, educational institutions and RP vendors should also adopt policies to protect whistleblowers who report privacy violations or security vulnerabilities in RP platforms.

• When enforcement actions are taken against test-takers suspected of academic misconduct, institutions must voluntarily share all information pertinent to that determination with the accused, including but not limited to the relevant data collected by RP technologies. Users of RP technologies should be especially mindful of relying upon the conclusions of AI systems to support claims of misconduct if the underlying AI technology has not been subject to rigorous peer review.

• Policies should be amended or adopted to address directly how collected data will be used to resolve allegations of academic misconduct, and how the institution will maintain compliance with FERPA and all other applicable laws and regulations. These policies should be freely accessible for students to review prior to course enrollment. Ideally, they should also be standardized within an institution or department.

SECURITY

• Security must be a primary design objective of all RP software. Accordingly, prior breaches of RP systems and reports that RP vendors have threatened or filed suit against individuals who have complained about their products are particularly troubling.


25 Indeed, the committee notes that outside the U.S., sole reliance on automated decision-making could well be illegal. See, e.g., Article 22.1 of the European Union’s General Data Privacy Regulation.

26 Institutions, for example, may have to modify their document retention policies to accommodate online class recordings, chats, and discussion boards to comply with applicable federal and disparate state laws.


• Institutions procuring RP software should require affirmative statements that vendors will not suppress warnings about defects in their products, will promptly disclose known product vulnerabilities, and will issue software updates as frequently as needed to minimize cyber risk.

• Vendors should adopt an affirmative public disclosure and bug bounty program, and commit to not use copyright, cybersecurity, or confidentiality claims to silence legitimate criticism, particularly from educators and students.

• As noted above with respect to privacy, RP technologies should incorporate end-to-end encryption for all test-taking data,29 both in transit and at rest.

ACCESSIBILITY

• RP vendors must ensure that their systems are accessible to all potential users, including users with disabilities and those who have limited equipment or internet connectivity.

• Test-takers who require special accommodations must be able to fully and equitably utilize RP technology. Institutions’ RP systems must allow the use of assistive technology and not inappropriately identify students making use of authorized accommodations.

• RP technologies should be designed to respect behaviors that may be suspicious in neurotypical test-takers, but may be involuntary in others (e.g., looking around the room). For institutions, this could require human adjudication of flagged behaviors. For vendors, this dictates that neurodiverse training sets should be used for automated systems.

EFFICACY

• Educators, researchers, and technology providers should develop uniform benchmarks and certification procedures to assess and document the comparative effectiveness of RP systems in identifying students receiving unauthorized help, whether with the aid of physical notes, other websites, or other people present at the testing location.

• Given that RP technologies depend on automated systems whose accuracy has often been proven to be substantially reduced by bias, particularly with respect to race and gender,30 such systems and the institutional policies governing their use must provide means to appeal determinations by automated systems to a human for re-adjudication.

• Vendors thus should train and test their software on a wide range of complexions, hairstyles, body types, etc., and publish the results of these tests for educational institutions, students,

---

29 Test-taking data includes responses, data collected as a result of monitoring, and test-taking metadata (such as IP addresses, mouse movements, and keystroke intervals).

30 See Note 4.
and independent researchers\textsuperscript{31} to review. Similarly, RP vendors should be required to test their software with both neurotypical and neurodiverse students. The committee also urges that questionnaires and all other user-facing materials intrinsic to RP software be gender neutral in their composition.

USTPC also recommends that practices, policies, rules, and statutes governing the development and deployment of all RP technology be consistent with its Statements on Algorithmic Transparency and Accountability,\textsuperscript{32} Joint Statement on Principles for Responsible Algorithmic Systems,\textsuperscript{33} and Statement on the Importance of Preserving Personal Privacy.\textsuperscript{34}

\textsuperscript{31} Given the broad impact that RP technologies are likely to have on academia and industry certification processes, and the millions of people engaged in them, the research community should monitor the adoption of RP technologies and, as the data may dictate, periodically make science-based recommendations for their refinement and use.

\textsuperscript{32} www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

\textsuperscript{33} https://www.acm.org/binaries/content/assets/public-policy/final-joint-ai-statement-update.pdf

\textsuperscript{34} www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0162
Comment on FR Doc # 2023-09353

Submitter Information

Email: [redacted]
Organization: The Retail, Wholesale and Department Store Union, RWDSU

General Comment

See attached file(s)

Attachments

OSTP_RFI_RWDSU_6.14.23
United States Office of Science and Technology Policy (OSTP)

Request for Information: Automated Worker Surveillance and Management

OSTP seeks comments to better understand automated surveillance and management of workers, including its prevalence, purposes, deployment, and impacts, as well as opportunities for Federal agencies to work with employers, workers, and other stakeholders to ensure that these systems do not undermine workers’ rights, opportunities, access, health or safety.

The Retail, Wholesale and Department Store Union, RWDSU, represents nearly 100,000 workers across the United States. The RWDSU organizes workers in apparel retail, grocery stores, food processing, meat packing, warehousing, cannabis, non-profits, nursing homes, carwashes and other low wage sectors. Many of these sectors that we organize in have implemented increasingly invasive forms of surveillance in the workplace, used to monitor worker productivity and occasionally to even harvest worker data that can be monetized. We agree with the use of technology to improve work and make it more efficient, but not if it dehumanizes workers, undermines the right to freedom of association, or comes at the expense of worker health and safety.

Below are several examples of how technology has been deployed in the workplace that we have seen in practice through our work organizing and representing workers. We do not use any names or identifiable information for the privacy of the workers who have experienced these issues. The deployment of the following technologies are primarily used at Amazon warehouses, although we know that Amazon is licensing and selling much of their worker surveillance technologies to other companies. This means that this technology is likely to be seen in many more workplaces in the near future.

- Monitoring by Robots: Many grocery stores across the United States have begun utilizing a robot, one such version referred to as “Marty,” in their stores to monitor inventory, identify hazardous situations like spills, and communicate with customers, but there is evidence that they are also monitoring workers themselves. These robots are equipped with cameras and also may have the potential to record audio, which may have a chilling effect on workers communicating amongst themselves.

- Termination by AI: Amazon utilizes the “A to Z” App for most of its human resources (HR) functions. Workers download the app to their personal phones. Often, this app represents the only relationship a worker holds with HR – there is no one they can talk to on site to address issues like PTO, wages paid, or other essential issues. This also means that there is often no human to call either – workers sometimes spend hours on the phone waiting for a human to pick up the phone to ask a simple question about their work and benefits. Some workers, after
spending hours trying to speak with an HR representative, are notified on the A to Z app that they have in fact been fired.

- Cameras Everywhere: Amazon warehouses are full of cameras. One accounting noted over 1,000 cameras in a single facility. These cameras, in combination with the handheld GPS devices, are used to monitor every aspect of a worker’s shift. One worker noted that when he was disciplined for making an error, management showed him a picture of him making the error, proving that these pervasive cameras are used for monitoring and discipline. These cameras as well as the radio-frequency handheld scanners were used to monitor social distancing by workers during the COVID-19 pandemic. Workers who were identified to have been within 6 feet of another worker were disciplined or fired for violating the social distancing policy. There were also legitimate concerns raised that these cameras were used to monitor voting during a mail-ballot union election at an Amazon facility. These cameras create fear among workers.

- Time Off Task Monitoring: Amazon uses a system called Time Off Task (TOT) as one measure of productivity. A worker who is not actively moving towards their next task is no longer on task. If a worker fails to be on task too many times or for too long of a time will be disciplined. TOT is measured by a radio-frequency handheld scanner that each worker carries. This device monitors movement and task completion. In some facilities, bathrooms are so far away from a worker’s work station that they are unable to travel to the bathroom and back without violating the TOT policy. This leads workers to either the unhealthy practice of not using the bathroom regularly, or sometime going to the bathroom in bottles.

- Quotas: Amazon also uses a form of work-place quota to monitor work productivity. This quota is based on the number of boxes moved or packed during a certain period of time. Quotas are tracked through radio-frequency handheld scanners and are algorithmically managed, meaning there is not a human monitoring productivity rates and adjusting them accordingly. Instead, there is an algorithm that monitors productivity rates and increases them based on the data points are used in the algorithm. Workers who fail to meet set quotas are disciplined.

It is also important to note that technology can also be used to obtain data on workers that violate worker privacy. Often it is impossible to know what is being collected and how it is being used behind the scenes by companies. What we do know is that workers provide ample baseline data to employers: resumes, biometric data such as fingerprints or iris scans, and workflow monitoring. Data from outside the company are also used by management in human resource decisions, such as social media history. As a matter of principle, workers should have access to, and influence over, data collected on them. There should be guiderails on data processing, the data minimalization principle should be enshrined in law, and workers should have the full right of explanation when data is used by a company. For a starting point in understanding this issue, please review the International Labor Organization’s Code of Practice for Protection of Workers’ Personal Data.
Technology, used to surveille workers for the purpose of management and discipline, is becoming more and more ubiquitous. The Federal government should consider rules about the overuse of technology to monitor and discipline workers, especially when such technology can be used for dual purposes, such as identifying and undermining union organizing campaigns.
General Comment

Please see the attached comment from the Economic Policy Institute regarding the Office of Science and Technology Policy's Request for Information on Automated Worker Surveillance and Management.

Attachments

epi-ostp-rfi-worker-surveillance
June 15, 2023

Alan Mislove
Assistant Director for Data and Democracy
Office of Science and Technology Policy
Executive Office of the President
1650 Pennsylvania Ave., NW
Washington, DC 20504

Re: Request for Information: Automated Worker Surveillance and Management

Dear Dr. Mislove,

The Economic Policy Institute (EPI) is a nonprofit, nonpartisan think tank created in 1986 to include the needs of low- and middle-income workers in economic policy discussions. EPI conducts research and analysis on the economic status of working America, proposes public policies that protect and improve the economic conditions of low- and middle-income workers, and assesses policies with respect to how well they further those goals. EPI submits these comments in response to the Office of Science and Technology Policy’s Request for Information (RFI) on automated worker surveillance and management.¹

The following comments are most relevant to these questions posed by the Office of Science and Technology Policy:

- What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers’ pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights? (Question 4b)
- What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers’ abilities to form and join unions and bargain collectively with their employers? (Question 4c)
- What data or evidence exists on whether automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination? (Question 4e)
- Where might further research, including by the Federal government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems? (Question 4k)
- Are there policy approaches to regulating automated worker surveillance and management systems from State, Tribal, territorial, or local governments or other countries that Federal agencies could learn from? (Question 5b)

To understand the prevalence of automated worker surveillance and management systems, one must consider the origins of worker surveillance and the rise of such systems over recent years.

Economic Policy Institute

Some of the earliest forms of worker surveillance can be traced back to times of slavery, where slave owners would keep meticulous records of the productivity of slaves and their profits. Over the years, the techniques used to track productivity of slaves have been used as the foundation for modern worker surveillance we see today. Fundamentally, the use of surveillance in the workplace is for employers to assert additional power over their workers.

Through both academic research and journalistic accounts, we know that automated work surveillance and management systems have been used to determine how workers are hired, what wages workers are paid, and when workers work, among other things. In theory, the use of automated systems has the potential of providing beneficial impacts for workers, such as providing workers with predictable schedules or reducing bias against workers during the hiring process. However, there is evidence that these systems have negatively impacted workers. For example, Amazon workers have cited being fired from their job from data gathered by a tracking system monitoring time workers are not directly working without the intervention of human supervisor. The use of automated facial recognition software have impacted workers of color ability to work remotely. The introduction of automated systems has shown to exacerbate “just-in-time” or “on-call” scheduling, which is found to cause stress and precarity for workers, especially those in the retail industry.

Automated systems have also been utilized to control the pace and speed of work or to monitor production quotas, either directly or indirectly. There is some evidence that technological advancements in these systems have also had harmful impacts for basic worker health and safety. A 2021 report from the Strategic Organizing Center examined workplace safety, injury rates, and safety policies at Amazon fulfillment centers, including the use of automated robotic technology to move and stock products throughout the fulfillment center. The report found that injury rates at Amazon facilities that used the automatic robots were higher than those without, and that workers faced increased risk of stress or injury due to the pressure of “keeping up” with their robot counterparts. A 2023 report surveying international Amazon workers found over half (51.7%) of surveyed workers agreed that Amazon’s performance monitoring had a negative impact on their physical health, and 57.3% agreed that this technology negatively impacted their mental health. Another recent paper from Veena Dubal documents how algorithmic wage-setting is replicating and exacerbating racial and gender wage discrimination amongst workers providing on-demand services through app platforms.

---

4 Annabelle Williams, “5 Ways Amazon Monitors Its Employees, From AI Cameras To Hiring A Spy Agency,” Business Insider, April 5, 2021.
5 Camille Anidi, a contract lawyer in Long Island told the Washington Post about her experience with a facial recognition software that her employers required her to use when working from home. The system, which has been shown to perform worse for people of color, often failed to recognize her face, and it sometimes mistook the Bantu knots in her hair for recording devices—forcing her to log back in and re-scan her face from three angles in order to accomplish the tasks expected of her. See Drew Harwell, “Contract Lawyers Face A Growing Invasion of Surveillance Programs That Monitor Their Work,” Washington Post, November 11, 2021.
7 Strategic Organizing Center, Primed For Pain: Amazon’s Epidemic of Workplace Injuries, May 2021.
Reports also show that automated worker surveillance and management systems are being used to monitor and ultimately discourage worker organizing efforts. For example, it was reported in 2020 that Amazon was investing in technology that would “track and counter the threat of unionization” at the company. According to a complaint filed by the National Labor Relations Board (NLRB), Google was accused of unlawfully terminating two employees who were in the process of organizing protests against the company. The NLRB alleged that the company illegally surveilled employees who viewed a union organizing presentation and interrogated others. These reports are concerning, because in addition to being a legally protected right, unions are a key tool for workers to rebalance the power they lack under our current economic system. While it is ultimately illegal for employers to surveil workers for supporting a union, research shows that employers are charged with making threats, engaging in surveillance activities, or harassing workers in nearly a third of all union election campaigns.

Fortunately, the National Labor Relations Board’s General Counsel has urged the Board to protect workers from electronic worker surveillance and automated management systems. In a 2022 memorandum, the NLRB’s General Counsel urged the Board to presume a worker’s Section 7 rights under the National Labor Relations Act are violated if surveillance or automated systems are present in the workplace and if they would interfere with efforts to unionize. In cases where the Board does not find the automated systems have violated workers’ rights, the General Counsel urges the Board to require employers to disclose to workers the type of data being collected, the purpose of its collection, and how it will be used.

Even with the NLRB’s recent efforts, there is little known about the type of data the employers are collecting from their workers and how employers are using the data to make decisions that impact their workers. For example, app-based workers routinely do not know how their wage rates are calculated. The use of automated worker surveillance and management systems also has impacts on work privacy. According to a report by Data & Society, Walmart managers have asked workers to download an app on their personal devices to assist with inventory, without mentioning that the app requires access to cameras and location services. In 2021, Walmart announced a plan to provide free smartphones to over 740,000 employees with the intention of being used at work. Although a company spokesperson said that the company would not have access to personal data, users signed an agreement which acknowledged that the device is subject to “monitoring, collection, retention, imaging and search as noted below, including any personal content that the user may place on device. Walmart may access the device, including remotely through the security app.” Further, employers often use third party vendors to help administer their automated systems with little

12 Celine McNicholas, Margaret Poydock, Julia Wolfe, Ben Zipperer, Gordon Lafer, and Lola Loustaunau, Unlawful U.S. Employers Are Charged With Violating Federal Law In 41.5% Of All Union Election Campaigns, Economic Policy Institute, December 2019.
14 Alexandra Mateescu and Aiha Nguyen, Algorithmic Management in the Workplace, Data & Society, February 2019
explanation of what data is being collected and how that data is being used. Federal policymakers should further investigate the type of data that is being collected by employers and third-party vendors and for what purpose that data is being used. For example, Senator Bob Casey recently urged the Department of Labor to explore available actions to research and recommend policy solutions to protect workers from exploitation through increased use of surveillance in the workplace. We support related efforts, such as this Request for Information from the OSTP, and the recent White House listening session with workers, to collect quantitative and qualitative data alike on how surveillance and automated management technologies are being used and encourage all relevant federal agencies to look for similar opportunities to take action.

Fortunately, some state governments are working to ensure automated worker surveillance and management systems are not negatively impacting workers, and can provide helpful models for similar guardrails at the federal level. In January 2023, California enacted laws that allow workers to know if their employers are surveilling them and why, what data is being collected, and give workers access to see, correct, or even delete such data. Further, California workers can opt-out of allowing their employers selling said data to third parties. In New Jersey, legislation has been introduced that would regulate automated hiring systems to minimize the chance of discrimination. The New Jersey bill would also require employers to notify job seekers whether they were using an automated hiring process. States are also working toward addressing the lack of transparency related to automated management systems and wage rates for app-based workers. In Colorado, legislation has been introduced that requires app-based companies to disclose to consumers and workers what portion of payments are going directly to the workers—who are often independent contractors without basic wage and hour protections—versus which portion of the payment is going to the company itself. Federal policymakers should enact similar policies to ensure that workers and consumers are not negatively impacted by the use of automated worker surveillance and management systems.

Sincerely,

Margaret Poydock
Policy Analyst and Government Affairs Specialist
Economic Policy Institute

Samantha Sanders
Director of Government Affairs and Advocacy
Economic Policy Institute

Monica Leon
Policy Intern
Economic Policy Institute

---

The Future of Work in the Age of AI: Displacement or Risk-Shifting?

Pegah Moradi and Karen Levy
The Oxford Handbook of Ethics of AI
Edited by Markus D. Dubber, Frank Pasquale, and Sunit Das

Print Publication Date: Jul 2020  Subject: Law, IT and Communications Law
Online Publication Date: Jul 2020  DOI: 10.1093/oxfordhb/9780190067397.013.17

Abstract and Keywords

This chapter examines the effects of artificial intelligence (AI) on work and workers. As AI-driven technologies are increasingly integrated into workplaces and labor processes, many have expressed worry about the widespread displacement of human workers. The chapter presents a more nuanced view of the common rhetoric that robots will take over people’s jobs. We contend that economic forecasts of massive AI-induced job loss are of limited practical utility, as they tend to focus solely on technical aspects of task execution, while neglecting broader contextual inquiry about the social components of work, organizational structures, and cross-industry effects. The chapter then considers how AI might impact workers through modes other than displacement. We highlight four mechanisms through which firms are beginning to use AI-driven tools to reallocate risks from themselves to workers: algorithmic scheduling, task redefinition, loss and fraud prediction, and incentivization of productivity. We then explore potential policy responses to both displacement and risk-shifting concerns.

Keywords: artificial intelligence, AI-driven technologies, workplaces, labor processes, displacement, human workers, AI-induced job loss, task execution, algorithmic scheduling, fraud prediction

IN February 2011, Jeopardy! viewers watched as the AI system known as IBM Watson defeated Ken Jennings and Brad Rutter, two of the winningest Jeopardy! champions of all time, in a three-day exhibition match. The New York Times lauded as “a vindication for the academic field of artificial intelligence.” Watson’s ability to understand and respond to Jeopardy! clues was considered a major step forward for natural language processing and information retrieval, and soon after, IBM announced plans to use the system to assist physicians in making diagnoses or treating patients.

Winning at Jeopardy! was a unique challenge for a machine, given that Jeopardy! is more unpredictable and complex than a simple test of trivia; as Jennings wrote in 2019, its clues are “weird, short little haikus, laced with hints, puns, winks, and red herrings.” When Watson erred, it often seemed to miss clues that humans would find easy or obvious. Watson, for example, rendered “what is chic?” in response to the clue “stylish ele-
gance, or students who all graduated in the same year"; Brad Rutter subsequently offered the correct response, "what is class?" In a Final Jeopardy! round with the category "U.S. Cities," Watson responded, "What is Toronto????" with four question marks denoting low confidence in the response.

But despite its shortcomings, Watson still won. Many assumed that this was simply because Watson had a memory capacity of fifteen trillion bytes and had been fed data from millions of documents, books, encyclopedias, and news articles. Watson was able to consume a wealth of information that most people—even Jeopardy! champions—could only dream of being able to absorb. But it is also possible that a much simpler mechanism gave Watson the biggest advantage of all: Jennings suggests that Watson was so good largely because it was much quicker to the buzzer than its human competitors were. "As Jeopardy devotees know," Jennings notes, "if you’re trying to win on the show, the buzzer is all. On any given night, nearly all the contestants know nearly all the answers, so it’s just a matter of who masters buzzer rhythm the best." In response to criticism over Watson’s buzzer advantage, IBM researcher Eric Brown noted: "there are some things that computers are going to be better at than humans and vice versa. Humans are much better at understanding natural language. Computers are better at responding to signals."

The combination of comparative strengths and weaknesses that Watson brought to the Jeopardy! stage nicely encapsulates the nuanced relationship between AI and human work. The computer’s success was seen as a bellwether, as futurists used Watson’s win as a launch pad for claims about the possibility of AI displacing workers. ("After all," fretted Martin Ford, "if a machine can beat humans at Jeopardy!, will computers soon be competing with people for knowledge-based jobs?") In some respects, Watson’s abilities were far superior to those of its human competitors—but humans were innately capable of aspects of gameplay with which Watson struggled. Though the specifics of the task may differ, the same is true of all human/machine relations in work contexts.

To understand the ethical issues most likely to beset the future of work, we must first realistically assess what kinds of threats AI might pose. Though some economists and policymakers have begun to express great concern about what AI will mean for employment—including whether some forms of work will exist at all—we argue that the popular “robots will take our jobs!” narrative of AI-induced job displacement is overly simplistic and alarmist. In spite of rapid growth in research and in application, AI systems still have quite limited practical capabilities, and the current technical limitations of AI still give humans the comparative advantage in many kinds of work. Forecasts of widespread employment displacement tend to focus solely on technical aspects of work, and neglect broader contextual inquiry about the social components of work, organizational structures, and cross-industry effects. In the first part of this chapter, we explain these limitations of existing forecasts.

In the second part, we turn to the outcomes we do expect from AI in the workplace. Specifically, intelligent systems are likely to be marshaled toward traditional man-
agerial goals related to efficiency, productivity, and risk mitigation. We highlight four ways in which firms may use AI in pursuit of these goals, effectively offsetting risks from themselves onto their workers. We end with discussion of potential policy responses to these concerns.

**AI as Worker Displacement: Rhetoric and Reality**

As AI-driven technologies are increasingly integrated into work processes, a commonly expressed concern is the impending displacement of human workers—often apocalyptically phrased in popular media as “robots taking over our jobs.” This argument tends to follow from the understanding that human work is comprised of a series of tasks, some or all of which can be done more effectively, efficiently, or at scale by a machine. Therefore, as machines grow in capability, a greater number of tasks currently performed by humans can (and, it is assumed, will) be automated. Because human work is comprised of these tasks, the thinking goes, human workers are vulnerable to being displaced by machines—potentially leaving many without jobs or drastically rearranging how labor is distributed by occupation. And because the jobs widely believed to be most acutely threatened by AI are blue-collar jobs—often held by less educated and poorer workers with fewer alternative options—there is, it is feared, potential for tremendous social and economic disruption.

**What Kinds of Tasks Can AI Execute?**

Machines are newly capable of performing a number of tasks formerly “off limits” to automation, thanks to technical improvements in AI, increased access to big datasets, and advancements in robotics. Prior to these developments, the paradigmatic model of task-based automation was the two-factor model proposed by Autor, Levy, & Murnane in 2003, which we will refer to as the ALM model. ALM focuses on how routine a task is on one dimension, and the degree to which tasks involve cognitive versus physical work on the other dimension. As Autor and his co-authors argued, “computer capital” could substitute for workers executing abstractable, programmable routine tasks—consisting of both “cognitive and manual tasks that can be accomplished by following explicit rules.” Watson’s buzzer advantage was rooted in this specific routine capability: being able to respond quickly and predictably to an explicit signal. The ALM model posited that nonroutine human labor might be complemented by computers, but that computers were unlikely to substitute wholly for humans for nonroutine tasks. Nonroutine tasks were deemed more difficult to program and dependent on skills like perception, problem-solving, and intuition that were well beyond the purview of computing in 2003.

But the world has changed since then. As computers have become more sophisticated and responsive to their environments, they can adapt to dynamic situations more adeptly—negotiating traffic, responding to conversational cues, developing novel solutions to problems. In light of robotic capabilities, computer vision, and machine learning, it’s less
important than it once was that a task be clearly definable and repeatable, thus complicating the ALM model. With AI, many tasks previously thought to be intractably nonroutine are becoming converted into abstractable problems aided by the availability of large and complex datasets.\textsuperscript{12} Although machines were previously limited to tasks that were clearly defined with limited potential contingencies, today’s AI systems can analyze previous cases to determine a course of action in unpredictable situations. Likewise, integrating prediction-driven models with robotics can bring these capabilities into the realm of physical labor. For instance, though Autor et al. explicitly mentioned truck driving as a manual nonroutine task in their 2003 work (and hence likely to be safe from automation), several companies have set goals to develop fully autonomous long-haul vehicles in the near future based on new technical capabilities.\textsuperscript{13}

While AI can allow a machine to execute tasks that would have previously been considered nonautomatable under the ALM model, AI still has significant technical and social limitations, some of which are acknowledged in the forecasting literature. Frey and Osborne consider three “engineering bottlenecks” when calculating the automatability of American occupations, identifying “perception and manipulation,” “creative intelligence,” and “social intelligence” as areas that elude technological capability.\textsuperscript{14} Levy identifies broader limitations, arguing that AI will be able to better compete against human labor in tasks that are (a) narrow, such that the data the models use contains most of the contingencies it could face in the future, and (b) structured, such that the machine can easily identify consistent patterns in the data.\textsuperscript{15} Much like the factors described in the ALM model, however, these boundaries are elastic; both future changes in the capabilities of AI-driven automation as well as in the nature of the tasks themselves will continuously shift the window of automatability.

Some forecasts peering through today’s window of automatability nevertheless predict grim outcomes for employment. In their occupation-focused model, Frey and Osborne calculated probabilities of computerization for 702 occupations by using administrative data about the task content of those jobs from the U.S. Department of Labor and having AI experts classify the tasks according to their technical automatability.\textsuperscript{16} The study estimated that 47 percent of U.S. jobs were at high risk (which they defined as a 70 percent chance) of automation within twenty years—and most of these in low-wage occupations. The Frey and Osborne forecast has been extremely influential, dominating the narrative in both the popular press and in subsequent academic work (amassing 3,600+ citations as of the time of this writing).

**The More Complicated Reality**

Risk calculations like Frey and Osborne’s are often used to predict massive unemployment due to advances in AI. But these forecasts are significantly more complicated than they are sometimes portrayed, in large part due to crucial nuances in how work is executed and how industries are organized. First, and most crucially, technological capability to automate certain tasks does not necessarily translate to the actual automation of those tasks, nor of the occupations that to date have been chiefly comprised of those tasks.
These forecasts tend to focus exclusively on technical feasibility, with no account of social, legal, political, or organizational factors. But technologies do not operate in social vacuums, and firms’ adoption and implementation of technologies are contextually dependent on factors like internal organization, institutional and regulatory landscapes, and degree of unionization, and other variables.

Importantly, social and political factors have historically affected the distribution of automation risk. In particular, race and ethnicity in the United States can affect whose work is protected from automation and whose is not. For instance, historically, although the artisans whose work was deskilled and automated in the first American industrial revolution were largely white, the dangerous, low-wage factory labor that grew as a result of industrialization was largely performed by immigrants and nonwhite workers. Likewise, when considering Frey and Osborne’s predictions in conjunction with racial and ethnic demographic data, it appears likely that white workers are disproportionately more automatable. But white workers continue to have greater social and political leverage along with higher labor market power, thus altering how these demographic groups could be affected by automation. For instance, the predicted polarization of the labor market into low-wage service work and high-wage “knowledge” labor is likely to have different outcomes depending on workers’ race or gender. During this polarization process, black and Hispanic workers competing with white workers for low-wage service work may experience greater job loss due to structural disadvantages like reduced labor market power.

Moreover, automation often leads not to the elimination of occupations, but to changes in their task composition. Using the same framework as Frey and Osborne, but focusing on time spent doing tasks that are capable of automation using current technology, a McKinsey analysis argued that fewer than 5 percent of American jobs can be “entirely” automated. The McKinsey model ultimately makes a convincing argument that AI portends redefinition of human occupations rather than the replacement of entire jobs. This redefinition has occurred repeatedly during previous periods of rapid technological change. ATMs are often cited as an example of the scale effects of new technology outweighing substitution effects of automation: ATMs did not wholly eliminate the need for bank tellers, but rather changed the tasks associated with the role and allowed for the cost-effective expansion of bank branches. As Autor describes in a seminal 2015 work, whether this will be the case in the current wave of AI-driven automation is dependent on a combination of factors like whether nonautomated, “complementary” tasks are easily available elsewhere in the labor market.

Finally, there are limitations to conceptualizing occupations merely as baskets of discrete executable tasks. Though we may distill occupations to their component tasks for purposes of analyzing them, anyone who has held a job knows that work depends on deep-seated human knowledge that cannot always be boiled down to rule-sets and protocols (even nonroutine ones). The anthropologist Michael Polanyi called this the tacit dimension of human knowledge—there are things humans know and do in the course of everyday life that evade easy categorization and can barely be articulated, let alone auto-
These dimensions of human work are hard to capture in economic models, but represent reasons it will be more difficult for machines to wholly assume the roles of human workers. One 2016 OECD analysis applied much of the framework of Frey and Osborne but used self-reported information on the things workers actually do in their given occupation, finding greater variation of tasks within an occupation as well as more groupwork and face-to-face interaction in jobs. This study ultimately estimated that only 9 percent of individuals were at high risk of automation within the next two decades, in contrast to Frey and Osborne’s much more dire forecast.

Another important complication to these forecasts is that they do not attempt to account for indirect forms of worker displacement that might be wrought by AI. These studies focus exclusively on the technical automatability of tasks within particular occupations, but do not account for broader industry-level effects that may more fundamentally restructure labor markets and types of work. A notable example is the booming growth of online retail, supported and enabled by implementation of intelligent supply-chain systems, and the subsequent “retail apocalypse” closing down brick-and-mortar stores across the United States. By one forecast, 75,000 stores are expected to close by 2026, while 25 percent of retail sales are estimated to take place online, up from 16 percent today. Moving retail online does not necessarily directly automate the tasks required from a department store sales associate, but rather eliminates the need for that role altogether, while potentially creating different jobs at other points in the supply chain. The ensuing importance of warehouses over brick-and-mortar stores also creates a space where tasks can be simplified in order to better accommodate the application of AI and robotics. For instance, because it is challenging for robots to safely pick up variable items that have an unpredictable weight or shape—something that comes instinctively to humans—e-retail companies like Amazon are implementing systems that use AI to build appropriately sized boxes around items rather than having a robotic arm pick them up and place them in a box. As Frey and Osborne themselves note, tasks can be changed to become more automatable; indirect unemployment due to AI often results in this task simplification, by taking people out of the equation and instead creating environments more amenable to machines.

Each of these limitations demonstrates a way in which the outcomes of these forecasts are more complicated than they initially appear. It is not clear to what extent AI will displace existing jobs. What is more certain and more imminent is that AI will impact the conditions of work. Rather than focusing on the quantity of displaced work, we ask here how AI might impact the quality of work for workers on the job, by considering how managers leverage intelligent systems to further firms’ objectives. Questions like these are less amenable to broad economic forecasting and breathless headlines—but inarguably, AI’s impact on workers in the here and now has less to do with displacement, and more to do with integration into existing labor structures and managerial practices. Specifically, as we discuss in the next section, AI’s primary effect on work in these contexts is to shift risks previously absorbed by firms onto workers.
AI as Risk Reallocator

Technology has long held the promise of making work more efficient. Technological advances in the workplace are vaunted for their ability to increase productivity, to incentivize “good” work behaviors, to find and eliminate bottlenecks, and the like. By measuring and monitoring and analyzing and predicting, the rhetoric goes, we can find waste, streamline processes, and eliminate superfluous work. The mantra of analytics is practically an article of faith among managers, who believe that data will reveal the secrets to greater profit margins. In this scheme, workers’ labor is an input to be collected, analyzed, and algorithmically optimized like any other. These practices are rooted in the principles of Taylorism, Fordism, and scientific management, each of which aimed to minimize wasted effort and maximize production through the fine-grained pacing and control of work processes.\(^{33}\) AI in the contemporary workplace follows in the footsteps of this ethos via intensive monitoring and predictive analysis of nearly all aspects of work tasks and the broader supply chain.\(^{34}\)

Does all this monitoring and analysis make the workplace more efficient? Maybe—but not necessarily because these practices are actually eliminating waste or increasing productivity. Instead, these technologies can insidiously hide work by offloading its burdens from a firm onto its (comparatively less powerful) workers. Lots of inefficiencies still exist in monitored workplaces, but AI-driven managerial practices redistribute the risks and costs of these inefficiencies to workers while serving a firm’s bottom line. We enumerate an illustrative (but nonexclusive) list of four such practices in the following.\(^{35}\)

**Staffing and Scheduling**

Traditionally, the risks of fluctuating consumer demand have been borne largely by the firm. Some hours at a store or restaurant, for instance, may be unexpectedly slow. Though managers ideally try to match customer demand to labor supply (i.e., workers on shift), they previously could do so only approximately, usually based on historical indicators like aggregate sales volume during a given period. This often meant that managers bore the risk of overpaying for excess labor capacity (i.e., wages) for unexpectedly slow periods.\(^{36}\)

Algorithmic technologies have changed the landscape of staffing and scheduling, however, transferring the burden of demand uncertainty from the firm to the worker. More sophisticated staffing algorithms integrate many more sources of data—including, for example, real-time customer traffic derived from in-store sensor networks, as well as external variables like weather—to predict customer demand and associated staffing levels, and to do so more dynamically. The result for workers has been a variety of “just-in-time” scheduling practices that introduce significant precarity and instability into the lives of low-wage workers.\(^{37}\) These include patterns like irregular and “split-shift” scheduling (i.e., having workers work multiple shorter shifts during periods of high demand, and clocking out in between—leaving that time unpaid); high-fluctuation work schedules (many hours one week, few the next); and short-notice scheduling, including “on-call” shifts (in which
workers must make themselves available for a shift but are notified only just prior to the shift’s beginning about whether they should come in). The effect of each of these practices is to destabilize workers’ livelihoods by interfering with nonwork activities—like school, childcare, or a second job—and creating severe financial stress, leading even to intergenerational cognitive harms. Moreover, these costs are disproportionately borne by women and workers of color, who occupy service positions at higher rates. While firms may lower labor costs due to reduced risk of overstaffing, the upshot of all of these practices is that the burden of the uncertainty of demand is shifted to the workers subject to scheduling systems.

**Defining Compensable Work**

As firms gain more visibility into and control over workers’ activities, they can more narrowly define work to include only very specific tasks and then pay workers for those tasks exclusively. Managerial technology allows firms to focus closely on what is considered essential to a job. The Fair Labor Standards Act (FLSA) requires employers to pay employees for time worked, but only for those activities that are considered “integral and indispensable” to the principal tasks of a job. Under this standard, courts have ruled several activities noncompensable, like commuting to work, waiting to go through required security screenings, and donning and doffing protective gear, even though the principal work tasks cannot, practically speaking, be completed without them. Though many workers (including most gig economy workers) are not covered by the FLSA, the law’s narrow framing of compensable work is conceptually instructive here. Algorithmic technologies may further circumscribe firms’ definitions of essential and compensable work, but they do not actually reduce the amount of work that workers do.

For example: drivers for Uber and other ride-share companies are paid only for the time they are actively transporting a passenger—not the time they spend driving around waiting for the app to alert them to a passenger nearby; not the time they spend driving to a pickup point; not the time they spend returning from a long trip out of town; not the time and expense required to clean their cars and offer amenities in order to get high customer ratings (which can impact the security of their employment). Because these undertakings are not seen as directly generating revenue for the company, they are unpaid. Of course, in reality, all of these tasks are part and parcel of doing the work of Uber driving, and the costs of that work (including both opportunity costs—the time the driver could be making money otherwise, or doing something else entirely—and direct costs, like gas and vehicle wear and tear) are borne entirely by the driver. Though this model of payment isn’t created by algorithmic dispatch—it has, for instance, long been a feature of the truck-driving labor model—the use of AI-driven platforms to support these industries broadens and exacerbates these effects.

Granular measurement capabilities can also be used to more explicitly recalibrate compensation schemes in favor of the firm. In 2015, for instance, Amazon changed how it paid some authors of books available on its Kindle platform. Because Amazon’s technology gave it visibility into exactly how many pages of a book readers actually read, it began
compensating authors on a per-page-read basis, rather than by the number of books downloaded—shifting the risk of a boring book to the author. Similarly, music-streaming services like Spotify pay artists on a per-track-streamed basis (where a track is “counted” when a listener plays it for at least thirty seconds), rather than by albums sold or tracks downloaded. In theory, compensation models like these reward popularity, and implicitly, quality—but in practice, the model is often blamed for “streambait” homogeneity in cultural production, as risk-averse artists conform to styles most likely to generate revenue under the algorithm.

Collectively, these trends more tightly circumscribe what is considered compensable work by “counting” certain tasks but not others. And by constricting what is considered compensable work and optimizing narrowly for it, AI-driven systems may increase the proportion of work that is considered residual and unworthy of payment, like producing an (ultimately unpopular) song, driving to a passenger pickup, or replenishing mints to ensure a high rating. Those work activities—what Craig Lambert has termed “shadow work”—don’t disappear just because they aren’t accounted for. Rather, these systems shift these risks and costs from the employer to the worker, who must internalize the very real labor that doesn’t “count.”

(p. 282) Detecting and Predicting Loss and Fraud

AI may also be used to redistribute the risk of deliberate damage or loss brought to an enterprise by employees purposively behaving against the firm’s interests. This often involves employees violating the law or the terms of employment—whether by stealing merchandise, embezzling money from company coffers, or sharing a secret recipe—or whistle-blowing to bring to light a firm’s illegal or unethical behavior. The principal-agent problem poses inherent risks to running a business, and employers have historically attempted to lower this risk through myriad low-tech and high-tech means. It is the norm for an employer to call references to determine the supposed character of a potential hire and perform background checks for previous criminal convictions. Employees dealing with sensitive or proprietary information are often required to sign nondisclosure and noncompete agreements. The risks are especially prominent in retail, where the product is directly handled by employees, often without supervision: according to the 2018 National Retail Security Survey, approximately 1.33 percent of retail sales—amounting to about $46.8 billion in costs to U.S. retailers—was lost to inventory “shrink,” with employee theft cited as the second-highest cause of shrink after external shoplifting. The costs of shrink make retail a natural adopter of loss-prevention technologies and techniques, from the use of CCTV cameras to the maintenance and creation of an industry-wide hiring blacklist of individuals suspected of theft.

Employers use AI to continue cracking down on the risk of deliberate damage, often by using technologies that continuously track and analyze worker behavior and activity. Loss prevention firms like Appriss Retail offer services that use AI to model employee behavior and flag unusual behavior that could be fraudulent or harmful to the firm. Outside of retail, companies similarly monitor employee activity, especially communications.
leaked list of phrases from 2008 shows Goldman Sachs flagging emails with lines like “clowns managing the fund,” “report the matter to the sec/nasd/nyse,” or “this won’t happen again” for scrutiny.\(^{55}\) London-based firm StatusToday continuously tracks electronic behavior and flags unusual activity, like an employee accessing files they don’t usually access or copying large numbers of files.\(^{56}\)

Loss and fraud prevention, and the use of AI in its service, may seem to be quite reasonable on the part of the firm; after all, few would condone outright theft, and firms seem justified in protecting their assets, ensuring regulatory compliance, and the like. Our goal is not to pass normative judgment on the propriety or advisability of these aims or practices. Rather, we discuss them here for two reasons related to risk-shifting and worker power. First, though these technologies are explicitly framed as reducing the risk to firms of workers’ deliberate malfeasance, monitoring workers for theft and fraud is often practically inseparable from tracking for productivity or efficiency purposes. The same platform advertised to minimize threats to a firm’s security can be (and often is) also used to ensure employees are maximally productive;\(^{57}\) concerns about fraud may be used as a pretext to justify an entire data collection regime, as has been the case in other contexts (e.g., state benefits provision\(^ {58}\)). We discuss productivity monitoring in more detail in the next section.

Second, preventing and detecting loss and fraud have specific implications for risk reallocation between firm and worker. These systems are often predictive, meaning that the harm of malfeasance has not actually happened yet. In other words, rather than mitigating actual loss \textit{ex post}, the employer is looking for potential harm \textit{ex ante}. This is a distinction with an important difference for workers. If systems’ predictive accuracy is poor, or if employers are especially risk-averse—say, in a weak labor market in which they have abundant potential hires—these systems may prevent many workers deemed “risky” from being hired at all. In other words, the risk of future deliberate damage is displaced from firms to potential hires. Employers have long based hiring decisions on heuristics that “mark” workers based on characteristics like race or prior incarceration, often making these workers effectively unhireable and precluding economic opportunity.\(^ {59}\) Greater use of predictive systems for loss and fraud prevention may further exacerbate these trends, especially for workers who are already disadvantaged. A further complication arises from the nature of the data in theft prevention databases, which are self-reported and shared among employers, often based merely on suspicion (i.e., without substantiation \textit{or} subsequent criminal charges) and very likely to be inflected with employers’ own biases. (In fact, concerns about the inaccuracies and lack of due process associated with inclusion in such databases have given rise to lawsuits alleging that their use may violate the Fair Credit Reporting Act.\(^ {60}\))

**Incentivizing and Evaluating Productivity**

Finally, intelligent systems are used to measure, assess, and incentivize workers’ performance in the workplace. Like loss prevention, concern about workers putting forth less than full effort is a feature of principal-agent relations; firms take many steps to incen-
tivize workers to expend more labor\textsuperscript{61} and, conversely, may punish workers for perceived shirking. Though worker surveillance for productivity maximization is nothing new, AI-driven systems may extend the practice into new types of workplaces—for example, workplaces like long-haul trucking, previously shielded by such collection by virtue of its geographic diffusion\textsuperscript{62}—and toward more invasive and fine-grained forms of monitoring.

Amazon, for example, has issued “inactivity reports” for its warehouse workers, detecting when workers temporarily stop moving (even for periods as short as one minute);\textsuperscript{63} it currently holds a patent for a wristband that tracks a worker’s movements and speed, buzzing with haptic feedback to direct the worker to the next item.\textsuperscript{64} Workers in Amazon warehouses have reported grueling pressures, including inadequate breaks for using the bathroom and meeting religious needs, and physical and mental health crises as a result of such strenuous conditions.\textsuperscript{65} Leaked corporate documents show that worker supervision and tracking—up to and including termination of employment for insufficient productivity—is handled by an AI-driven system.\textsuperscript{66} Platform-based firms like Uber also use AI to promote driver productivity, using fleet-wide supply/demand predictions and behavioral-economic “nudges” to tailor incentives toward profit maximization.\textsuperscript{67} In customer-facing service jobs like call centers, AI can be used to monitor not only the speed of work but also alignment with behavioral and affective criteria like tone of voice. In retail settings, workers may be incentivized and evaluated based on automated analysis of their interactions with customers on the floor.\textsuperscript{68}

Productivity incentivization is not \textit{a priori} bad for workers; in commission-based work, for example, it may be advantageous for labor as well as management. But in many contexts, fine-grained monitoring erodes trust, dignity, and any sense of privacy from work, reduces workers’ decisional autonomy,\textsuperscript{69} and opens the door to labor exploitation by driving workers to the limits of their physical and mental capabilities. If working to less than one’s full capacity is considered a form of “time theft,”\textsuperscript{70} similar concerns attach here as they do with respect to loss prevention.

As we have described, intelligent systems in the workplace can be used in the service of several managerial techniques. They may enable firms to dynamically schedule workers, minimizing labor costs while creating substantial instability in workers’ lives. Firms may use AI to narrowly redefine work tasks, concomitantly classifying some practically necessary labor as ancillary and noncompensable. They may use it to predict worker theft and malfeasance, potentially resulting in an underclass of “marked” workers deemed too risky to hire. And they may use it to incentivize productivity by removing all slack from work time, perhaps doing serious damage to workers’ physical and mental health. These dynamics were not created by AI; they have been features of labor/management relations for a long time and will likely remain so for a long time to come. But AI may enable firms to more effectively pursue their existing goals through these practices, therefore offloading burdens and reallocating risks from themselves onto workers.
Displacement, Risk-Shifting, and Policy

Policy recommendations for the future of work commonly focus on mitigating the harms of labor displacement, like unemployment, depressed wages, and increased inequality as a result of labor market polarization. And although AI is often framed as a new frontier for policymaking, proposed solutions often focus on strengthening long-standing social institutions. These recommendations include investing in both K–12 and college education (often with a focus on STEM [science, technology, engineering, and mathematics] fields) and retraining displaced workers to provide them with marketable skills for the new economy; bolstering the social safety net through reforms to unemployment insurance and public benefits programs; and (somewhat more controversially) some support for universal basic income programs that would provide unconditional cash guarantees for all individuals, regardless of circumstance.

These policy proposals stand to benefit millions of Americans whether or not their jobs are displaced by AI and represent sound economic investments in the future of work—whatever it may look like. In addition to proposals like these, however, we should also consider what protections we might provide for workers who retain jobs, in order to temper risk reallocation that intensifies management/worker inequity. For example, a number of states and municipalities have taken steps to curtail worker-unfriendly scheduling practices through fair scheduling laws—sometimes in response to the threat of wage theft lawsuits. These laws do things like require managers to announce schedules further in advance, end “on-call” shifts, and create minimum shift lengths. In so doing, they help to recalibrate employers’ ability to shift costs to workers through algorithmic scheduling.

Other worker protections could similarly reallocate some risks back to firms. One clear avenue would be an end to forced arbitration, which often bars employees from litigating claims against their employers in court; proposed reforms like the Arbitration Fairness Act would prevent employers from being able to enforce arbitration agreements in employment disputes. A second route forward includes reforms to worker classification regimes that characterize many platform-based workers as independent contractors rather than employees, therefore removing some protections due to them under labor law (minimum wage, unionization, etc.); such reforms are currently afoot in some states. More broadly, amendments to the Fair Labor Standards Act could be made to include some workers currently exempt from its protections (for example, long-haul truck drivers) —and in some regulated industries, compensation regimes might be modified to more accurately recognize workers’ time and effort. And we might regulate or ban the use of for-profit “retail justice” databases that blacklist potential employees suspected of theft without due process.

One further note is in order. Organizational sociologists have long examined technological interventions into workplaces and their effects on workplace roles and relationships. A key lesson from this work is that technology has no unified set of effects once deployed in a workplace: it can alter new social dynamics or ossify old ones, depending on the conditions surrounding its deployment—including industry structures, broader economic
forces, workplace culture, and institutional mechanisms for governing relations between labor and management. These studies of previous technologies provide a vital lesson: Contemporary forecasting of AI’s impact on workers, and the ethical issues it is likely to bring to the fore, must include concomitant consideration of specific social, economic, and cultural dynamics in a workplace. Any policies put in place to mitigate negative effects must also take these into account. While this observation is a caveat for forecasters and policymakers, it is also cause for optimism: it suggests that there are many firm-level levers that may mitigate the negative dimensions of workplace AI, and that nothing is set in stone.

Perhaps contrary to our call for workplace-specific action, many of the aforementioned policy proposals we identify—in either the displacement-remediation or risk-reallocation buckets—may seem like they are too general, too basic, or have little to do with artificial intelligence specifically. This is because the issues resulting from integrating AI with work are not wholly new, but are instead the continuation of a long line of labor concerns that have endured and transformed throughout the history of industrialized work. But the specter of AI in the workplace does not necessarily spell doom or dystopia; rather, it elucidates the burdens placed on workers, and may bring new energy to creating policies that protect workers for generations to come—ultimately protecting the quality of work, not just its quantity.

Acknowledgments

The authors gratefully acknowledge support from the John D. and Catherine T. MacArthur Foundation, New America, and the Cornell University Center for Social Sciences. We are grateful for helpful comments and insights from Joshua Popp and Matthew Sun.

Bibliography


**Notes:**


(22) Moradi, “Race.”.


(26) Autor, “Why Are There Still So Many Jobs?”


(32) Brishen Rogers, “Beyond Automation: The Law & Political Economy of Workplace Technological Change,” February 4, 2019, https://papers.ssrn.com/abstract=3327608. Rogers reaches a similar conclusion in his analysis of the law and political economy of workplace automation. Like us, he posits that the threat of automation-induced job loss is “overstated” and that the more pressing issues involve managerial techniques, including worker monitoring and algorithmic scheduling. Rogers also thoughtfully points to the relation of workplace data collection to the “fissuring” of the workplace—that is, firms’ outsourcing of key functions to outside contractors.


(35) We focus here on management of already-hired workers, and bracket from our analysis consideration of AI’s emerging role in hiring processes. The implications of AI for hiring are ably analyzed by Miranda Bogen and Aaron Rieke in “Help Wanted: An Exploration of Hiring Algorithms, Equity, and Bias” (Upturn, Dec. 2018), https://


Levy and Barocas, “Refractive Surveillance.”


Vega v. Gasper, 36 F.3d 417 (5th Cir. 1994).


Llorca v. Collier County Sheriff, 898 F.3d 1319 (11th Cir. 2018).


(55) Eamon Javers, “You Won’t Believe What Gets an Email Flagged at Goldman: CNBC Has the List,” CNBC (June 16, 2016), https://www.cnbc.com/2016/06/15/you-wont-believe-what-gets-an-email-flagged-at-goldman-cnbc-has-the-list.html. Though the list cited is from 2008 and was rather low-tech in execution, Goldman Sachs has continued this practice with updated search terms.


Levy and Barocas, “Refractive Surveillance.”


---

**Pegah Moradi**
Pegah Moradi, Department of Information Science, Cornell University

**Karen Levy**
Karen Levy, Department of Information Science, Cornell University
June 15, 2023

Re: Request for Information: Automated Worker Surveillance and Management

Submitted electronically via the Federal eRulemaking Portal at regulations.gov
Docket No. OSTP-TECH-2023-0004

Pegah Moradi, Cornell University Department of Information Science
Dr. Karen Levy, Cornell University Department of Information Science

We submit the below comments in response to the Office of Science and Technology Policy’s Request for Information seeking public input on automated worker surveillance and management. We applaud OSTP’s efforts to protect workers’ rights and opportunities via this Request for Information and related activities.

We submit our comments from our perspective as researchers actively involved in examining the effects of worker surveillance, algorithmic management, and the use of artificial intelligence technologies in the workplace. Pegah Moradi is a PhD student in Information Science at Cornell University, where she is a National Science Foundation Graduate Research Fellow. Moradi’s research focuses on how data-driven automation affects economic life, with a focus on how data-driven automation affects workers. Dr. Karen Levy is an associate professor in the Department of Information Science at Cornell University and associated faculty at Cornell Law School. Levy researches the legal, social, and ethical dimensions of data-intensive technologies, particularly in the context of labor and work. Levy is a New America National Fellow and a Fellow of the Canadian Institute for Advanced Research. Levy holds a J.D. from Indiana University Maurer School of Law and a Ph.D. in sociology from Princeton University, and is the author of Data Driven: Truckers, Technology, and the New Workplace Surveillance.

Below, we respond to select questions from the Request for Information pertaining to:

4a) What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers’ pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

4c) What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers’ abilities to form and join unions and bargain collectively with their employers?

4h) What data and evidence exist on why employers decide to adopt automated worker surveillance and management systems?

4i) Are there any existing or new systems that aggregate worker surveillance data across multiple employers?

4k) Where might further research, including by the Federal government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?
5c) What policies or actions should Federal agencies consider to protect workers’ rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

4a) What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers’ pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

Effects on Worker Pay:

By collecting granular data about workers at scale, firms may be able to more narrowly define what counts as compensable work, paying workers only for what the firm deems necessary tasks (but excluding a good deal of work which is realistically necessary for performing the job). The effects on pay may be most pronounced for hourly and gig workers for whom pay is more tightly linked to accomplishing discrete tasks or reaching certain milestones: Uber drivers in most jurisdictions, for instance, are paid only for when they are transporting a passenger, even though their work necessitates other time-consuming tasks, like waiting for the app to assign them a passenger, driving to a pick-up spot, or cleaning and maintaining their vehicle. Upwork, a prominent freelancing platform, requests freelancers being paid hourly to set up software on their computer that allows Upwork to capture screenshots of their computer screen at random and record workers’ clicks, scrolls, and keystrokes. The client can then view the screenshots and usage data in a “Work Diary” and dock a freelancer’s pay if the data reveals the user isn’t exclusively focused on work tasks during a given time period.

Moreover, data-driven workplace tools that allow for closer supervision of workers tend to lead management to devalue worker experience and knowledge, relying instead on insights from data to judge whether workers are making optimal decisions or performing their duties appropriately. In Dr. Levy’s ethnographic study of the long-haul trucking industry, for instance, the real-time availability of data on trucks and road conditions often eroded trust in truckers’ on-the-ground judgment about how to conduct one’s work safely.

Relatedly, automated surveillance of consumers can have downstream effects on workers, a phenomenon known as “refractive surveillance.” In retail environments, for instance, clienteling software can be used to identify high-value and repeat customers, assign workers a specific personalized script or process for these clients, and centralize information previously held by individual workers. By routinizing work that typically requires training, knowledge, and experience into discrete tasks and centralizing workers’ knowledge in a database, more experienced workers may lose their bargaining power in the workplace and become more readily substitutable for one another.

---

We further note that digital tools can make it difficult for workers to ameliorate wage theft problems, substantiate wage discrimination claims, and remedy other violations of compensation agreements. When compensation schemes, job assignments, and other material conditions of work are determined through opaque algorithmic management processes—as they often are, for instance, in platform-mediated labor contexts—workers have very little transparency to understand why they received the treatment they did, and have little recourse to address these issues. Similarly, the use of time and attendance software can sometimes exacerbate wage theft issues by obfuscating managerial decisions and imposing default rules that reduce worker compensation.

**Effects on Worker Benefits:**

A majority of Americans (54.3%) use employer-provided health insurance. While some federal laws protect employees from medical discrimination, many Americans still have a vested interest in keeping their personal medical information private from their employer, so as to keep their employment and their access to healthcare. And though employers are typically prevented from accessing employee health data without express permission, an array of data-driven tools allow employers to learn about their employees’ health through legal means. In particular, employers can contract with technology vendors to run workplace wellness initiatives, allowing the vendors to access and analyze employee data, and providing employers with inferences about employee health without any access to protected patient records.

Use of employee health information can occur on an individualized level: Walmart, for instance, contracted with a healthcare analytics company, Castlight Health, to scan employee insurance claims and infer which workers were more likely to pursue costly medical care: Employees who stopped filling prescriptions for birth control, for instance, could be pregnant; employees receiving treatment for back pain might pursue expensive spinal surgery. Though Walmart itself did not access the individualized data, Castlight flagged employees that would then receive personalized messages to nudge them towards certain healthcare decisions (like receiving physical therapy in place of spinal surgery) that are at lower cost to the insurance company.

While these individualized effects exist, given legal constraints and heightened privacy norms around personal health information, vendors tend to only provide aggregated data on

---


employees to firms. But aggregating data still poses potential inferential harms for workers.\(^9\) Aggregation does not guarantee privacy or anonymity, especially in smaller firms, and aggregated data can still be used to make inferences about individual employees’ health, regardless of whether or not their data was included in the original dataset.\(^10\) One pregnancy tracking app, Ovia, assuages workers’ fears of privacy intrusions by only sharing aggregated data (including data on high-risk births and pregnancies) with employers. But Ovia’s business-facing marketing materials focus on how tracking can help pregnant employees return to work as quickly as possible, and aggregate data on high-risk pregnancies at work can help employers know how they can most effectively change coverage if necessary.\(^11\) Just as with pay, more granular tracking of workers’ personal lives allows employers to avoid some of the otherwise accepted risks of conducting business, including providing ample healthcare for employees.

**Effects on Employment:**

Workplace surveillance can contribute to long-term changes in employment. As discussed above, fine-tuned measurement of workers and work environments can *deskill* occupations by distilling them into their component tasks and devaluing workers’ expertise. An extension of this process is using data collected from workers in order to inform the design and development of automation that can perform these tasks in place of humans. This is especially true for gig workers: Janet Vertesi and coauthors find that multiple firms that invest in “contract labor networks”—such as Amazon, for delivery drivers, and Uber, for rideshare drivers—simultaneously invest in developing technologies to eliminate the need for these workers altogether, like delivery drones and autonomous vehicles.\(^12\) Automated management and using distributed, contracted workers allows these companies to expand their operations and data collection at scale without taking on the typical costs of employing a large workforce. As a result, firms are able to invest in automation long-term, with precarious employment outcomes for the workers hired in the interim.\(^13\)

Like worker data, *consumer* data collection can similarly help to help create systems that automate tasks. And other labor-saving technologies that offset work tasks to consumers, such as self-checkout, require firms to surveil customers as if they were workers. In self-checkout in

---

10 Solon Barocas and Helen Nissenbaum, “Big Data’s End Run around Anonymity and Consent,” in Privacy, Big Data, and the Public Good: Frameworks for Engagement, ed. Helen Nissenbaum et al. (Cambridge: Cambridge University Press, 2014), 44–75, https://doi.org/10.1017/CBO9781107590205.004. Barocas and Nissenbaum refer to these sorts of downstream effects of data collection and analysis as the “reachability” of an individual, as opposed to an individual’s personal identifiability in a dataset.
particular, retailers must implement surveillance infrastructure to prevent customers from stealing merchandise at checkout. Implementing automated surveillance systems for customers and workers alike may ultimately end up displacing work tasks and leading to long-term changes in employment across occupations and sectors.\textsuperscript{14}

**Effects on Physical and Mental Wellbeing:**

Surveillance systems are often implemented with the stated intention of promoting worker safety and wellbeing. Retail stores assert that they implement surveillance cameras in part to protect workers from customer abuse and violence,\textsuperscript{15} and many firms install technologies to monitor delivery and truck drivers for signs of fatigue to prevent accidents and keep drivers safe on the road.\textsuperscript{16} But worker monitoring technology is often a double-edged sword, and worker protection rationales often justify the use of technologies that can also be used to police and punish workers, eroding autonomy in how they do their jobs and posing risks for retention of an experienced workforce.\textsuperscript{17}

Conversely, automated monitoring of workers can lead to more unsafe work conditions, as tracking that incentivizes productivity and punishes idle time can drive workers towards the point of physical and mental exhaustion in order to meet various metrics. Amazon has issued “inactivity reports” for warehouse workers, detecting when workers stop moving for periods as short as one minute and giving workers “penalty points” if they are flagged as having spent too much time off task.\textsuperscript{18} Amazon workers have subsequently reported intense pressures at work that have led to unsafe working conditions, including inadequate bathroom breaks and mental breakdowns.\textsuperscript{19} Some workers have even called the Amazon warehouse a “Lord Of The Flies’-esque environment where the perceived weakest links are culled every year.”\textsuperscript{20} Workplace wellbeing and electronic monitoring are thus tightly linked: In a survey of call-center workers conducted by the Communication Workers of America union, workers who reported “high

---


\textsuperscript{17} Levy, *Data Driven*; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (Picador, 2019).


electronic monitoring, high frequency of formal discipline, unreasonable performance metrics, and unfair compensation practices” reported the highest levels of stress.\textsuperscript{21}

Automated management systems can also lead to mental wellbeing harms by creating a more precarious quality of work that can be destabilizing to workers’ livelihoods. Staffing and scheduling algorithms, including “just-in-time” scheduling, analyze patterns of demand and schedule shifts accordingly. These shift patterns may be irregular, short, or “split”—where workers clock in for multiple shorter shifts during periods where there are bursts of demand\textsuperscript{22}—leading to detrimental effects on worker health and well-being that extend intergenerationally.\textsuperscript{23} In an ethnography of workers at fast-fashion retail stores, Madison Van Oort finds that high employee turnover and volatile schedules meant even managers did not fully know who worked at the store—leading firms to emphasize the need for further algorithmic management as workers "came and went too often to be kept track of ‘the old-fashioned way.’"\textsuperscript{24} Van Oort refers to the additional burdens of working under digital monitoring and volatile algorithmic scheduling as the “emotional labor of surveillance,” a “less obvious form of emotional labor [that] helps keep the store running.”\textsuperscript{25}

Lastly, productivity tracking and data-driven management can be dehumanizing and frustrating to workers, especially in forms of frontline interpersonal work or occupations that have strong norms of personal autonomy. The \textit{New York Times} reporting on productivity monitoring highlighted some of these cases, like a hospice chaplain who received “points” for attending funerals, calling grieving families, or visiting dying patients.\textsuperscript{26} In long-haul trucking, truckers consistently report that being digitally monitored made them feel like criminals or like children, and that invasive camera and biometric monitoring reduces the dignity that drew them to the profession.\textsuperscript{27} These reductions in worker wellbeing are, critically, more than hurt feelings or sour grapes on the part of workers encountering new managerial dynamics; they also pose critical risks to worker retention and recruitment in economically and socially essential workplaces.

\begin{footnotesize}
\begin{enumerate}
\item\textsuperscript{21} Virginia Doellgast and Sean O’Brady, “Making Call Center Jobs Better: The Relationship between Management Practices and Worker Stress” (Communication Workers of America, June 2020), https://ecommons.cornell.edu/handle/1813/74307.\textsuperscript{6}
\item\textsuperscript{24} Van Oort, “The Emotional Labor of Surveillance.”\textsuperscript{25}
\item\textsuperscript{25} Van Oort.
\item\textsuperscript{27} Levy, \textit{Data Driven}.
\end{enumerate}
\end{footnotesize}
Broader Questions of Productivity:

Finally, it is questionable whether technologies intended to measure and improve productivity actually do so, as monitoring technologies record work tasks that are easy to track—but these are often not the tasks that are most meaningfully productive. Workers frequently take on additional unproductive tasks in order to meet metrics and make themselves legible to tracking. This often looks like busy work, like jiggling a mouse so it’s registered by monitoring software, or doing quick but meaningless tasks that are countable by monitoring systems—like sending several emails—rather than deeper but less quantifiable engagement. Ethan Bernstein’s study of workers at a major mobile phone factory found that workers have to take extra, costly steps to conceal their behavior from tracking. The study found that small increases in the privacy of groups in the factory improved those groups’ performance on the assembly line, in what Bernstein calls the “transparency paradox”: Managers’ attempts to make workers more observable counterintuitively makes the workers less effective in their roles.

4c) What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers’ abilities to form and join unions and bargain collectively with their employers?

There have been a variety of high-profile cases of employers purportedly using automated surveillance, contextual data, and digital traces to directly predict and prevent worker organizing:

- Leaked Whole Foods memos showed the firm calculated a unionization “risk score” for each store based on a variety of metrics, including employee turnover, racial demographics, OSHA violations, and local unemployment rates.
- Some Google employees claimed the firm was attempting to detect organization efforts through internal tools that alerted management if an employee created a calendar event with a large number of rooms or participants.
- Amazon corporate tracks social media posts from Amazon Flex drivers in closed Facebook groups intended only for Flex drivers, and explicitly categorizes posts having to do with “Strikes/Protests” or warehouse complaints.

Employers can also prevent organizing indirectly. Many of the forms of surveillance and algorithmic control that we discussed in response to question 4a (and discussed further below in response to question 4h) also create conditions that make it difficult for workers to organize. For

instance, scheduling workers in short, irregular shifts makes it difficult for workers to develop trusting relationships during shifts or take breaks at similar times. If workers are tightly monitored and punished for idle time, they are less likely to find time to organize. And if managers are able to track workers beyond the walls of the workplace—for instance, through access to workers’ emails and texts or by keeping tabs on workers’ social media behavior—workers have fewer places where they can organize outside of their employers’ gaze. Geographically distributed and remote work similarly make it more challenging for workers to organize, and make work stoppages less effective.33

4h) What data and evidence exist on why employers decide to adopt automated worker surveillance and management systems?

Employers adopt automated worker surveillance and management systems in order to lower costs and shift the risks of conducting business from the firm to its workers. (We outline the mechanisms behind this risk-shifting process in greater detail in our chapter in The Oxford Handbook of Ethics of AI, “The Future of Work in the Age of AI: Displacement or Risk-Shifting?” which we have attached to this comment.)34 Employers adopt systems like surveillance cameras, productivity trackers, and digital correspondence monitoring in order to avoid costs. Likewise, algorithmic scheduling and predictive analytics aim to forecast future worker and consumer behaviors, whether that’s making a particular sale to a particular kind of customer, asking for a raise, looking around for another job, or joining a union campaign. This kind of predictive management is attractive to firms that ultimately want to minimize the risks and unknowns of business.

Firms may also be motivated to adopt worker surveillance and management systems based on motivations related to perceived consumer desires. Consumers may, for instance, demand greater visibility into supply chains (driven by industry norms): In a service context, consumers increasingly want to be able to rate workers’ services, track packages, or predict when a pizza is likely to be delivered. These motivations can be used to justify worker surveillance by managers.35

An additional driver of employer adoption of these systems is their low cost and wide availability. Increasingly, capture of workers’ behaviors and communications is already built into common office software products, like Microsoft Office or Zoom, that companies are already using; using these tools for worker analytics poses little additional cost or burden to managers.36 Data are


34 Moradi and Levy, “The Future of Work in the Age of AI.”


36 Kate Kaye, “Companies Are Using AI to Monitor Your Mood during Sales Calls. Zoom Might Be Next.,” Protocol, April 13, 2022, https://www.protocol.com/enterprise/emotion-ai-sales-virtual-zoom; Alex Hern,
easy to capture, passively and continuously, throughout the workday. This ready availability stands in contrast to previous managerial strategies that required greater resource outlays to monitor workers.

Finally, the rise in remote and hybrid work arrangements post-pandemic has been a strong catalyst for broadened worker surveillance. As workers no longer do as much of their work in physical offices co-located with managers and colleagues, managers are increasingly anxious about worker productivity and potential shirking, leading them to deploy new tools to gain visibility into workers’ behaviors (for example, keystroke tracking, attention monitoring, screenshots, webcam access, and other capabilities).³⁷

4i) Are there any existing or new systems that aggregate worker surveillance data across multiple employers?

Some systems for aggregating data across employers are relatively low-tech, but still relate to data sharing across firms: Some retail companies subscribe to databases of employees that are suspected of stealing from the store, regardless of whether the suspicion was substantiated or whether the individual faced criminal charges. Multiple retailers use these databases (which are often maintained by background-checking firms) in the hiring process, effectively blocking certain individuals from being able to work in retail altogether.³⁸ Concerns over the lack of due process in these cross-employer databases have led the FTC to investigate whether their use violates the Fair Credit Reporting Act, though it ultimately declined to recommend enforcement action in one such case involving a database maintained by LexisNexis.³⁹

In other cases, aggregated data from vendors can be shared across employers in order to compare their own firm’s performance to that of other firms. In trucking, for instance, some fleet management systems generate driver “scorecards” that can facilitate comparison of performance between individual drivers and fleet and industry averages.⁴⁰

---

⁴⁰ Levy, Data Driven.
**4k) Where might further research, including by the Federal government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?**

We suggest three areas of further research:

1. **Multidisciplinary research on geographically distributed work:** Firms are increasingly applying automated surveillance systems to previously “off-limits” workforces — such as long-haul truckers, remote workers, and freelancers. For remote workers especially, employers can now permeate the boundaries between the home and the workplace. How do these workers respond to new forms of tracking, and how do these systems affect the quality and dignity of their work?

2. **Multidisciplinary research on frontline work:** Likewise, frontline workers are often under high scrutiny from surveillance and automated management systems, often because they work with customers that are also being surveilled by firms. Further research should consider how new data-driven technologies mediate the interactions between customers and employees, ultimately affecting how frontline workers now must work among technologies.

3. **Labor market impacts of surveillance technology:** Data-driven systems are often used to justify hiring contracted workers (“fissuring” the workplace) or train labor-saving technologies. While much economic research focuses on macroeconomic labor market trends due to automation, there is still little research on how workplace fissuring and automation affect employment outcomes across industries and within firms. In particular, there is still little understanding about how these outcomes might differ for different racial and ethnic demographics throughout the U.S.

**5c) What policies or actions should Federal agencies consider to protect workers’ rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?**

We describe some policy recommendations in our attached chapter (“The Future of Work in the Age of AI: Displacement or Risk-Shifting?”). In summary, effective policies to support workers can take multiple forms: They can involve strengthening existing workplace protections (such as the Occupational Safety and Health Act) and enacting new labor protections, like living wages for gig workers, ending forced arbitration, reduction of worker misclassification in the gig economy, or new rules around the collection and use of workplace correspondence for anti-organizing efforts.

Protections for workers can also be incorporated into omnibus privacy legislation and regulations: In the U.S., there is no federal worker privacy law, and omnibus privacy protection bills have tended to focus on consumer privacy rights, excluding employees. We echo Alvin

---


Velasquez’s call to include workers within the ambit of proposed omnibus privacy legislation, and to draw upon the full capacities of the FTC and NLRB to protect worker privacy.45

Most crucially, we suggest that the strongest tool for protecting workers’ rights and wellbeing involves strengthening the social safety net overall: If surveillance and automated management make workers’ livelihoods more precarious, then strengthening and expanding social institutions like unemployment benefits, public health insurance, and public education can allow for workers to have greater economic stability regardless of the circumstances of their employment. Such measures should involve strengthening protections for especially vulnerable populations, like those in the ADA, Title XII of the Civil Rights Act, and the Pregnancy Discrimination Act.

Many of our policy suggestions may not seem specific to new technologies, but workplace surveillance issues are not wholly new or unique: Concerns about ensuring safety, autonomy, and dignity in work have existed throughout the history of labor in the U.S. The use of new data-driven tools brings these historical tensions to a brighter light, perhaps bringing greater energy and momentum towards enacting policies that promote the wellbeing of all workers.

Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0164
Comment on FR Doc # 2023-09353

Submitter Information

Name: Pegah Moradi
Address:
Email: [redacted]

General Comment

See attached file(s)

Attachments

Attachment1_Moradi_Levy_OSTP_RFI_Comment
Attachment2_The_Future_of_Work_in_the_Age_of_AI
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0165
Comment on FR Doc # 2023-09353

Submitter Information

Email: [redacted]
Organization: Electronic Privacy Information Center (EPIC)

General Comment

Please find attached comments of the Electronic Privacy Information Center (EPIC)

Attachments

EPIC-Comment-OSTP-RFI-Worker-Surveillance-Letter
COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

White House Office of Science and Technology Policy

on

Request for Information: Automated Worker Surveillance and Management

88 Fed. Reg. 27,932

June 15, 2023

The Electronic Privacy Information Center (“EPIC”) submits these comments in response to the White House Office of Science and Technology Policy ("OSTP")’s Request for Information posted on May 3, 2023. OSTP is soliciting comments on the impacts of automated worker surveillance systems such as “risks to workers, including to their health and safety, equal employment opportunities, privacy, ability to meet critical needs, access to workplace accommodations, and exercise of workplace and labor rights, including their rights to form or join a labor union.”\(^1\)

The Electronic Privacy Information Center is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and

\(^1\) https://www.federalregister.gov/documents/2023/05/03/2023-09353/request-for-information-automated-worker-surveillance-and-management
litigation. EPIC has consistently advocated for the right to be free from the effects of inaccurate, biased, or otherwise harmful scoring and screening techniques.

EPIC applauds OSTP’s continued focus on the harmful impacts of new and emerging technologies, including automated worker surveillance. As its comment, EPIC submits its 2019 complaint to the Federal Trade Commission against job applicant screening company HireVue and provides a suggested reading list of important work on worker surveillance, both by EPIC and other authors. EPIC’s complaint against HireVue highlights both the harmful use of facial recognition on job applicants and the inherent risks of unleashing algorithmic decision-making systems without enacting safeguards.

Today’s surveillance of workers and job applicants inflicts at least two kinds of harms. First, pervasive surveillance is bad for workers, allowing companies to deny workers’ rights to break time, reasonable accommodations, and organizing and by increasing stress through ultimately unhelpful productivity monitoring. This same invasive monitoring denies workers human dignity and their right to privacy. Second, automated monitoring and evaluation systems are likely to make mistakes, falsely flagging workers as unproductive or applicants as unsuited because algorithmic decision-making systems are often inaccurate and discriminatory. EPIC urges the OSTP to take a broad view of worker surveillance and consider the multiplicity of harms created by surveillance, both when it works as intended and when it goes off the rails. EPIC also urges OSTP to define worker surveillance broadly to include surveillance in the hiring process.

---

2 EPIC, About Us (2023), https://epic.org/about/.
Suggested Reading on Worker & Job Applicant Surveillance


- Algorithmic Decision-Making Generally:

- State of Worker Surveillance Today:

- Similar Harmful Surveillance Practices:
  - Complaint of EPIC, In re Online Test Proctoring Companies (Dec. 9, 2020), https://epic.org/documents/in-re-online-test-proctoring-companies/

Respectfully Submitted,

John Davisson
John Davisson
EPIC Senior Counsel
Jake Wiener
Jake Wiener
EPIC Counsel

Thomas McBrien
Thomas McBrien
EPIC Law Fellow
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0166
Comment on FR Doc # 2023-09353

Submitter Information

Email: [Redacted]
Organization: International Federation of Professional and Technical Engineers

General Comment

See attached file(s)

Attachments

IFPTE Comment RFI OSTP 15June2023
June 15, 2023

Dr. Arati Prabhakar  
Director and Assistant to the President for Science and Technology  
Office of Science and Technology Policy  
Executive Office of the President  
Eisenhower Executive Office Building  
1650 Pennsylvania Avenue Washington, D.C. 20504

Submitted Electronically

Regarding: Request for Information, “Automated Worker Surveillance and Management,” Federal Register No. 2023-09353

Dear Director Prabhakar:

On behalf of the International Federations of Professional and Technical Engineers (IFPTE) – a labor union that represents upwards of 90,000 professional employees working in the federal government, in the state and local public sector, in aerospace and defense, energy, and the nonprofit sector – we thank you for the opportunity to respond to the Office of Science and Technology Policy’s (OSTP) Request for Information on “Automated Worker Surveillance and Management.”

IFPTE appreciates OSTP’s interest in this matter as it directly supports the Biden Administration’s commitment high quality jobs and workforce development, protecting working Americans’ right to join unions and bargain collectively, and ensure our nation is advancing high labor standards and equity throughout the labor market.

IFPTE’s response to this RFI also connects OSTP’s interest in worker surveillance to the Biden Administration’s commitment to making the federal government a model employer, providing fair and equitable delivery of government services, and enhancing transparency and public trust.

For IFPTE members employed in federal government, workplace surveillance and algorithmic management can create perverse incentives where quantity is prioritized over quality of work through performance appraisals based on metrics. This has significant negative implications for federal employees whose work duties involve compliance, fact-finding, and administrative adjudication proceedings. Those negative implications not only impact workers, but also present challenges to the delivery of quality public services, fairness and due process, and ethics and accountability in government administration.

Union members represented by IFPTE who preside over administrative adjudication proceedings at the Social Security Administration (SSA) and the DOJ’s Executive Office of Immigration Review’s (EOIR) Immigration Court have experienced problematic time-based performance-linked metrics. These production quotas -- the equivalent of a line
speedup -- are inappropriate as they undermine independent decision-making, impartiality, and due process. It creates a conflict between these employees’ duty to provide fair and impartial rulings in a timeframe dictated by the circumstances and facts of each case before them and performance appraisals and ratings linked to time-based production quotas.

IFPTE Perspective on Data Analytics and Algorithmic Management at the Social Security Administration’s Office of Hearing Operations

SSA administrative law judges (ALJs) are appointed under 5 U.S.C. § 3105. ALJs are part of the Office of Hearing Operations (OHO) at SSA and conduct hearings under the Social Security Act and pursuant to the APA, see 5 U.S.C. §§ 551 and 552. ALJs conduct due process hearings that are closed to the public due to the sensitive nature of the medical records involved. SSA ALJs ultimately adjudicate cases worth hundreds of millions of dollars each year. ALJs at SSA are members of IFPTE’s Judicial Council 1, and the bargaining unit is alternately referred to as the Association of Administrative Law Judges (AALJ).

ALJs are held to high ethical standards of conduct both in and outside of work and have statutory and regulatory responsibilities to exercise independent judgement, to avoid even the appearance of impropriety, and to ensure fair adjudication for the American people. Despite these heightened expectations, ALJs are subjected to frequent and secretive automated surveillance and data collection that has had significant negative impacts on our morale, engagement and service to the American people. These surveillance methods include:

- cameras in our non-public hearing rooms;
- surveillance of Microsoft Teams chat and/or audio/video conferencing;
- surveillance of email;
- Skype data collection and/or surveillance;
- VOIPPhone surveillance;
- time and attendance data collection and surveillance;
- keyboard stroke recording/detection;
- automated software designed by SSA to measure and evaluate employee performance; and
- data analytics tools that drive management decisions to the exclusion of context, and which result in managers abdicating responsibility.

The full extent of workplace surveillance and algorithmic management that takes place at SSA generally or in OHO specifically is not known. There are some guardrails in the AALJ-IFPTE collective bargaining agreement (CBA) on outright surveillance in the hearing room and through use of employees’ laptop cameras, but beyond that, the nature and extent of SSA’s surveillance is largely unknown.

Negative Impacts of Over-Reliance on Data Analytics

Over the past decade, SSA has increasingly and often exclusively relied on data analytics to assess workload performance. In part, this shift to a data-driven, goals-based employee management strategy has been in response to persistent staffing shortages and an attempt to force more work out of already over-burdened employees. SSA’s unrelenting focus on data collection and aggressive performance targets has demoralized its workforce and resulted in declining customer service. This rigid performance structure has created perverse incentives; instead of work units engaged in teamwork to accomplish the
Agency’s mission, employee focus is instead on individual and position-related production targets.

The negative impacts of this hyper-focus on data analytics have shown up starkly in the federal agency rankings compiled by the Partnership for Public Service’s Best Places to Work in the Federal Government. The 2022 rankings place SSA in last place for large agencies.1 This is in stark contrast to 2011, when SSA secured the number two spot for large agencies. In 2022, SSA had an employee engagement and satisfaction score of 53.9 out of 100. In contrast, the Agency’s highest-ever employee engagement and satisfaction score was 71.6 in 2010. In 2022, the Agency’s score in the “teambuilding” category ranked 14/16 for large agencies and its score in the “customer service” category ranked 12/14 for large agencies.

Data Manipulation/Unsupported Data

SSA has several publicly known programs that use data analytics to measure and review employee performance. These programs often rely on the measurement of inaccurate/irrelevant data and create incentives that erode the underlying data integrity. Some areas of concern include:

- **HowMIDoing and HowMIDoing Plus** is described as an ALJ workload management tool. Input from ALJs into the program was largely after the fact, and there are also concerns about data accuracy and reliability. For example, the tool does not count ALJ availability properly. Rather, ALJ availability is based on the fiction that all ALJs are available the same number of days—249 days, instead of the number of days an ALJ is actually available (i.e., accounting for leave taken, any training, administrative tasks, official time for union work, etc.). As a result, the average days in a particular case status goes up as soon as an ALJ goes on leave. Further, having the incorrect availability skews other data points, such as the average number of cases ALJs dispose of on a daily basis. Attached is a letter outlining the union’s concerns that was sent to the Johns Hopkins University Applied Physics Laboratory, with whom SSA contracted with the enhance the HowMIDoing tool.

- **DWPI (Decision Writer Productivity Index)** provides a performance metric for decision writers that attempts to account for the complexity of a case in determining an appropriate time allotment for the attorney advisors who assist ALJs in preparing decisions. There is no accuracy or quality metric within the index. Yet, this data ties directly to the decision writers’ performance evaluations and monetary bonuses thereby creating incentives to favor production over quality. Good public service requires that these goals are balanced. Notably, SSA does not solicit input from ALJs regarding the quality of the draft decisions and as noted quality is not incorporated into the index.

- **SSA’s Office of Appellate Operations (OAO)** houses the appellate body that reviews ALJ decisions—the Appeals Council. OAO reviews both random samples and “select” samples based on certain case characteristics it has deemed contain problematic issues or fact patterns. OAO’s 2023-2024 Strategic Work Plan indicates their goal of reviewing, in addition to a random sample of decisions, 1,000 “selective” samples. In theory, OAO states that data analytics are shared

with other agency components and are used to help make data-driven changes to policies and procedures. In practice, OAO does not transparently share the criteria for “selective” review with the ALJs whose cases are reviewed, either before or after the sample is complete. Likewise, they do not reveal whether the review showed that, in fact, the particular “problematic issue or fact pattern” did show an increased rate of error. Further, they do not reveal if there are any safeguards to ensure a particular ALJ or office is not targeted by the review sample. Likewise, a data point used by the Appeals Council to rate ALJ decision quality – the Appeals Council agree rate – is a volatile data point due to the statistically invalid sample size.

- **Timeliness metrics lack nuance but are nonetheless so critical to SSA management that the underlying data integrity is at risk.** In a July 2018 report, GAO concluded that the SSA’s main timeliness metric – average processing time (APT) – lacked nuance and that the agency should develop a set of metrics that more accurately reflect office performance. The report notes that the SSA’s Division of Workload Management (DWM) is charged with monitoring workloads. GAO notes that DWM holds calls with each regional management team to discuss the status of each region’s older (aged) cases and facilitates workload transfers. Anecdotally, the union has learned that the pressure to meet these workload goals results in cases being moved from one case processing status to another, not because the criteria for the new status is met, but because the pressure to move the cases is too great. In turn, this erodes the integrity of the underlying data used in the metrics, and as noted by GAO, the API already lacks sufficient nuance to accurately reflect an office’s performance. The attached letter to Johns Hopkins contains other instances of data inaccuracy and manipulation.

Collectively, the above noted programs obviously have some utility, but they lack nuance and transparency. Without that, the extensive reliance on these metrics is misplaced, especially since the validity of the data cannot be confirmed and/or these systems are prone to data manipulation. This increases employee stress and decreases job satisfaction, and certainly correlates with the Agency’s fall to 17th of 17 government large federal government agencies in job satisfaction.

**Production Demands United from the Complexity of Work**

It is concerning that efforts to use algorithmic metrics are focused on the highest skilled employees. Highly skilled government workers should be protected from the efforts to mechanize the most complex work that is critical the public, and the Agency should not automate, or abdicate, their management duties to opaque metrics.

In OHO, aggressive and unfounded case production targets have impacted every aspect of the hearing process. ALJs are overwhelmingly pressured to “produce numbers” despite the complexities of the individual cases before them. For over a decade, ALJ production quotas have been fixed and have not shifted in response to case complexity or even time available to work. This quota was reached without an analysis of the time needed to properly adjudicate these complicated cases. A 2021 GAO report found that ALJs are not given enough time to conduct a conscientious review of the record and that SSA has never

---

provided documentation or a rationale as to how SSA established its case deposition quota. SSA’s own internal training modules have undermined its unsubstantiated production demands – mandatory unconscious bias training and research support the principle that slower, more deliberate and intentional ALJ decision-making reduces the influence of inappropriate unconscious bias, ensuring that claimants receive a full and fair hearing.

Negative Impacts of Surveillance

SSA has not been transparent about whether, how, and why it engages in automated data collection and surveillance. While employees, including ALJs, have at times received vague warnings that we are being tracked, the union has not been provided any information about which systems or actions are being tracked, who has access to the surveillance data, when and why such data is accessed, and whether and how long the data is stored. This uncertainty has fostered a widespread belief among employees that they can be tracked doing almost anything in and around the office and has created an environment of fear and anxiety. This heightened level of anxiety and fear has had meaningful impacts on employee performance and on employees’ physical and mental well-being. Employees who are preoccupied with being watched and who document their work to defend against potential scrutiny are not able to fully engage with their work. Employees who already feel targeted by management due to speaking out, having been involved in an Equal Employment Opportunity or grievance action, or who feel vulnerable due to any number of protected statuses are especially impacted.

IFPTE Perspective on Data Analytics and Algorithmic Management at the Department of Justice Executive Office of Immigration Review’s U.S. Immigration Court

In 1983, the Executive Office of Immigration Review (EOIR) was created to oversee and administer the U.S. immigration court in response to perceived or existing conflicts of interest caused by immigration judges having to report to the same supervisors as the government’s immigration prosecutors in the previous structure. The design of the immigration court is a result of deliberate decisions by Congress and the Executive Branch to provide protection to safeguard the independence of the immigration judges and to free immigration adjudication from the law enforcement priorities of the immigration enforcement agencies. Immigration judges are hired as Department of Justice attorneys who are then appointed by the U.S. Attorney General to exercise independent judgment and discretion as administrative judges.

However, the previous Administration demonstrated how agency policy encroach on judicial independence by limiting tools available to immigration judges to fairly manage their dockets. Additionally, through the use of performance metrics and “case management tools,” policies could produce outcomes by reducing immigration judges’ independent decision-making to a semi-autonomous role.

Performance Metrics Dashboard

The DOJ implemented a digital performance metric dashboard during the last administration. It was a disaster and generated widespread concern because it emphasized

---


production quotas and time-based deadlines over judicial competence. The data was faulty, it brazenly drove a law enforcement agenda sacrificing judicial independence, and it institutionalized measures which were unattainable for the vast majority of the judges. The implementation of this mandate did not direct judges how to rule on a given case, but it penalized immigration judges when they took the time necessary to explore factual disputes, analyze complex or nuanced legal arguments, or delve into process issues of a given case and thereby fall behind the administration’s speed requirements. The quotas are punitive in nature and harm procedural due process by incentivizing truncated hearings, preemissions of applications for relief, and the denial of continuances.

While the current administration has rolled back the problematic measures, it still uses the dashboard to track judicial achievements on these legacy metrics. Given the lack of transparency, the judges do not know how these measures are being used to evaluate their performance. There’s a continuing need to develop a robust process for engaging employee representatives to implement this technology since the dashboard results continue to be a condition of continued employment to some degree.

**Deskilling Concerns about Technology**

The current administration has implemented a Judicial Tools (JT) application to aid judges on the bench as they preside. Unfortunately, JT was created without input from its end-users -- the trial judges. It is often unavailable due to bandwidth issues and raises ‘deskilling’ concerns since the judges now prepare and serve their own orders. Furthermore, JT has serious limitations for judicial responsibilities, as it does not have real-time evidence sharing capabilities, for example, where parties can upload, review, and present case documents during trial, and judges can’t make ‘sticky’ notes on documents as they review the file for later discussion during a hearing. The continued implementation of this technology would benefit through developing a system for regular engagement with employee representatives.

**Utilization of Technology to Address Health and Safety Concerns**

The pandemic forced state and federal courts across the country to quickly pivot to online hearings to ensure they could continue to meet their missions. The immigration courts did not. It took seven months before the immigration courts began to allow even a handful of judges to conduct hearings remotely. When faced with the crisis of the pandemic, the DOJ appeared to have neither the ability nor the will to adjust. Judges and staff around the country were required to hold hearings in person and the courts had to close repeatedly to address predictable health and safety concerns. Today, the court has a tranche of laptops that enable judges to hold hearings remotely, called DAR Laptops. Only about 20 percent of the corps have been issued such laptops, and there are indications that the court is reducing access to this tool, despite its demonstrated effectiveness, and appeal to the judges, as well as the parties -- DHS Trial Attorneys and private bar counsel -- that appear before it. Once again, developing strong structural engagement between agency management and employee representatives could be a successful way to ensure health and safety concerns are addressed efficiently and adequately.
Thank you again for the opportunity to comment and for considering our input. Our union looks forward to OSTP’s continuing our engagement with organized labor and we endeavor to be a resource to the Administration’s efforts to center workers and worker empowerment in our nation's policies regarding technology and the future of work.
Hello, I provided this file but I made a few errors & needed to finish removing the company name. Please use this file instead of the file uploaded at 5:00 pm today. Please DELETE the file already uploaded earlier at 5:00 pm Thank You

Attachments

EEOC CHG Shortnd 2 yr discrim pattern _030121_Final_NO NAMES_Final
Note: Names have been removed.

Employer: ABC Indian Outsourcing Corp. of US jobs to India and Guatemala

Disabled employee: Jane Doe

Here is the “Shortened explanation” of the conditions of the disability discrimination, harassment, hostile work environment & retaliation that has continued as a pattern of practice over the last 2 years from when I was working with ABC Corp. from about October 8, 2018 thru September 10, 2020.

Please Note: these events are True & a charge was filed with the EEOC but was ignored for legal continuation leaving the disabled worker alone without help and having difficulty for retention of Legal representation. Plus the US court system does NOT provide ADA accommodations and assistance for disabled workers.

The US Government NEEDS to create a “DISABILITY HARASSMENT” LAW WHICH IS SIMILAR TO THE SEXUAL HARASSMENT HR 4445 LAW WHICH WOULD END FORCED ARBITRATION OF DISABILITY HARASSMENT CLAIMS!!!!

----------------------------------------------------------------------------------

This is a long story of a continued pattern of disability discrimination, hostile work environment, harassment and retaliation over the last 2 years beginning with the 3rd week of employment back in late October 2018. This pattern of discrimination and retaliation for my filing 2 complaints with Human Resources in November 2018 and June 2019 continued all through 2019 and through 2020.

Due to the Limitations of the email file contents, I will give you a “shortened summary” of the events.

-------

This charge includes:

1) Disability Discrimination in a systemic continuing pattern of Practice over a 2 year time period with failure to accommodate, exclusion and marginalization, harassment, hostile work environment, and Retaliation with the unlawful release of my medical disabilities, then senior
management conspired and aided and abetted to cover up their unlawful release of my medical information to all working employees in the department.

2) Violation of ADA Laws & exclusion on the basis of disability, then later repeated retaliation and also “the forcing into a job that puts me in direct harm with my disabilities” while (ABC Corp) allowed Non-disabled employees NOT to work collections/ call center environment = direct conflict of my disabilities. When (ABC Corp) had Knowledge of my disabilities at all times. Plus (ABC Corp) did not force other Indian employees working in the US on an HB-1 Visa to the Collections job.

3) Systemic pattern of practice that when a “Job is Outsourced to India or Guatamalla, etc.” and the time period is over, then instead of laying off employees, (ABC Corp) intentionally forces workers into positions where it conflicts with their disabilities as with retaliatory intent to terminate the worker. This way (ABC Corp) does NOT have to pay the state’s “Retraining for laid off workers” as with what is the standard. (ABC Corp) uses a False narrative as to “systemically WHY a worker is terminated” without allowing the worker to view or respond to what the “Hidden reason is”. If they maintain some form of Artificial Intelligence tracking on “Incidents” then each and every worker NEEDS to VIEW and be able to RESPOND as to WHAT the actual reason is because as I pointed out MULTIPLE TIMES, the Foreign workers, whether in Guatamalla or elsewhere, even management, I have “Identified MULTIPLE instances where the foreign trainer/ management has ACTUALLY INFORMED WRONG INFORMATION IN THE TRAINING PROCESS, and then excluded me and later fired me for “ACTUALLY IDENTIFYING THAT SPECIFIC OPERATIONAL TRUTH” (ABC Corp) kept managers and foreign trainers that actually Instructed in training with WRONG INFORMATION OF A PROCESS and terminated others. If the EEOC obtains lists of all the “Hired & Terminated workers”, and then speaks to all the terminated workers, the EEOC will be able to uncover a systemic pattern which can be a CLASS ACTION against (ABC Corp)

4) Systemic use of Artificial Intelligence software to be “used as a basis of exclusion” without any pre-informed “quantifiable measurable means of job tasks” but when any non-disabled people made errors they were ok.

5) Systemic discrimination by the use of Artificial Intelligence software to be “used as a basis of exclusion” also without any pre-informed “quantifiable measurable means of job tasks” of “domestic & disabled workers” are NOT informed nor shown any “quantifiable measurable means of job tasks” as for foreign Indian and Guatamalin employees were actually “favored for job training, advancement, pay raises, and special projects and bonuses.” As I have been told by management that I was “Excluded from the payroll tasks on 11/27/2018 “Because I repeatedly requested an ADA accommodation” LATER (after Management CHANGED their reason of WHY I was Excluded on 11/27/2018 from the payroll tasks), in June 2019 after my 2”nd complaint to HR, I was later told a different answer of “Why I was excluded from the work tasks for 7 months from 11/27/2018 thru June 2019, Management said that “I was TOO SLOW” as compared to the other non-disabled workers. However there was NEVER any measurable means shown or tracked to be able to view, Thus (ABC Corp) has a Systemic use of Artificial Intelligence
software to be “used as a basis of exclusion” without any pre-informed “quantifiable measurable means of job tasks” but when any non-disabled people made errors they were ok.

I was working for (ABC Corp) in PA from about 10/08/2018 (?) thru 09/10/2020. (ABC Corp) uses Artificial Intelligence programming to work with Major US companies and streamline the corporation’s internal processes therefor allowing for United States workers Jobs then to be OUTSOURCED to foreign countries like INDIA & GUATAMALLA etc. etc. (ABC Corp) has grown immensely over the last say 16-17 years and has outsourced thousands and thousands of US jobs to foreign workers by a systemic discrimination continuing pattern of practice internal process against domestic United States workers and US disabled workers. (ABC Corp) has hired US workers, discriminated against them in a constant continuing retaliatory action, systemic pattern of practice and violated practically all of the US labor laws and retaliated against the US workers, including myself with my disabilities and terminated workers (ABC Corp) while additional workers from US Corp 500 companies are also being fired for the streamlined processes while does NOT maintain the same standard of "employee evaluation of work tasks" between US domestic workers as compared to it's foreign and also "HB-1 VISA imported foreign workers". (ABC Corp) always systemically discriminates and retaliates against the US domestic workers with training, pay, benefits, bonuses, and advancement, etc etc. As I will easily be able to demonstrate a 2 year pattern of practice of their many many repeated US violations of practically all Labor laws.

I have maintained a thorough timeline of all the events and can show a continuous pattern of practice over the 2 years. I have been excluded from job tasks for 7 months, subjected to mocking an ridicule, denied training, denied ADA accommodations for my disabilities on repeated occasions. I have filed 2 complaints with (ABC Corp) and participated in the investigations and seen how they cover up events and promote the Managers who lie and unlawfully release my personal medical information to all of the workers subjecting me to the continuing hostile work environment. They have denied me a $3000.00 bonus because I would not sign a "employment discrimination release from charges" form. Thus because again of my disabilities, I was not paid for the work bonus, while non-disabled workers were paid the bonus. I did the work but was not paid it, only for the fact of I refused to sign the: “General Release from employment discrimination form”. All of the other workers were paid the bonuses. I have a lot of detailed events for the continuous action. They also violated FMLA laws too. This has the potential of being possibly a class action lawsuit, if the EEOC decides to obtain documentation of: "all the employees hired & then fired" by this company over the last few years.
I was hired 10-8-2018 for payroll processing. I have previously had 13 Yrs ACH and payroll processing with a local community bank. I have worked "Back Office operations" and NEVER as a "Call Center position" which requires the constant use of a Headset and constant phone communications which is a direct conflict with my lifelong disabilities for which (ABC Corp) HAD KNOWLEDGE OF AT ALL TIMES SINCE THE END OF OCTOBER 2018!!!

My disabilities are: "MERLD" = Mixed Expressive Receptive Language Disorder, and "CAPD" = Central Auditory Processing Disorder and I have Tinnitus = Ringing of the ears.

When I was Hired back in October 2018 for Payroll Processing of a payroll, the job was "Outsourced to India" around March of 2020, right at the time of the COVID-19 Pandemic. (I need to send in a more "detailed" timeline of specific events but I will summarize it for you)

**Shortened Historical Summary of some events:** (Incomplete, as not to bog you down, the exact “incident by incident action over a timeline” is too much to include within this email.)

In October 2018, there were 3 managers (Mngr1, Mngr2, Mngr3) (Mngr3 quit in May 2019) whom would CONSTANTLY TELL CONTRADICTORY WORK TASK INSTRUCTIONS for the payroll process and expected NO NOTES to be used. Towards the end of October 2018,(around October 25th 2018 +/- a few days) AFTER a group training, and AFTER everyone Left the closed training room, I asked to speak with two of the managers alone & in private; (Mngr1 & Mngr2). While the 3 of us were in a “PRIVATE" room and within a closed door office, I disclosed my disabilities to them & asked for the “Accommodation of: PRINTING OUT MY NOTES to be able to retain large volumes of new tasks.” I provided them with the medical documentation and requested as the primary accommodations for my “ability to create and modify my own notes in writing and to be able to print out my notes.” My shift at the time was
9:00 am to 5:30 pm and everyone else arrived at an earlier shift and was in by 8:00 am for their scheduled time. (I was to work with a client in Colorado in a different time zone, that’s why I started later) The NEXT MORNING, Mngr2 told all the people in the department that I was "Learning Disabled" and then both Mngr2 and Mngr1, LIED AND HID THAT FACT FOR MONTHS, Until I had a "WITNESS" willing to testify whom informed me of what they did. I immediately starting being subjected to mocking and ridicule from most of the departmental personnel, and at the time I didn’t know that the Managers were ACTUALLY THE ONES whom disclosed my disabilities. A few months later a co-worker told me what management had done (Told everyone I’m learning disabled the next day) and she said she would be willing to testify in court as to their actions. I was being called stupid, and it will take me all day to do one task, the co-workers would laugh at me and talk behind my back, thus I filed the first complaint with ABC Corp Human Resources in the Winter 2018. Both Mngr1 and Mngr2 LIED TO COVER IT UP WHICH IS AIDING AND ABBETING UNDER THE LAW. This was a very hostile work environment at ABC Corp.

My requests for disability accommodation went ignored for over a month (fall 2018) while I was subjected to the mocking and ridicule. I patiently waited and on 11/27/18, I again asked Mngr1, if he could provide me with "whom I should contact about getting disability accommodations for my requests" for printed notes and within 1 1/2 Hrs from my written Instant Message that I sent to Mngr1 request, asking "whom I should speak to", he immediately tapped me on my shoulder and said that I was not doing payroll anymore. He "REMOVED ME FROM THE PAYROLL WORK TASKS" and said that "I had TO WAIT for the ADA ACCOMMODATIONS TO BE COMPLETED” before I could do the work tasks. My Accommodations didn’t occur until about January 22, 2019. However I was STILL removed from the payroll work tasks until early June 2019 when I filed my second complaint with HR. This REMOVAL FROM WORK TASKS WENT ON FOR 7 MONTHS LONG !!! I was mocked and ridiculed practically DAILY because of this and subjected to a hostile work environment for the entire 2 years that I worked at ABC Corp. I made my 1st complaint around 11/28/18 to the HR rep. and I informed them that out of these 3 managers, each of them would tell me a "DIFFERENT INSTRUCTION" and that their instruction was constantly contradictory of what was informed earlier. When I would "Write down" the instruction, and then point out that "this is how I was instructed" to do something and then a different manager of the 3 would say to do the process a different way. I would constantly "Point this out" and it just upset them because I could factually substantiate the task. For example; Later when I was processing payroll, they would have excel spreadsheets/ containing employee Hours which had to be reformatted to CSV and Uploaded for the Processing of requested time off. I was Instructed to contact the client for any "Awaiting Approvals" of Paid Time Off requests because previously my client had been negligent in actually "Approving" the PTO, which meant that the hotel would delay - "at the last minute of the pay week" the entire pay file because they would "WANT ALL of the Awaiting Approval employee's PTO - to be: APPROVED". Thus, it meant I would have to input say 30-50 PTO's at the last minute & hold up the payroll. Thus for Months, I would contact the client's manager regarding these "Awaiting Approvals". Then later a different manager would instruct me that "I was NOT following the process" and NOT to input the PTO requests resulting in the 30-50 employee's NOT being Paid for their requested Time OFF. This would only result in MORE problems for the following pay week bece then there would be MORE corrections necessary. This is just one example of many which went on for a year and a half. I also complained of their "step by step instructions" (SOP's) that they wanted us to
follow would be wrong and was NOT updated properly and would constantly "Re-direct a person out to 8 different areas, and frequently containing wrong information and wrong instruction, which was time consuming" and the instructions could be easily restructured into a much more shortened direct instruction. I would give them suggestions which were ignored. Later, by the time practically the entire first group of employee's quit and a new bunch of employees were hired and all of them had the same problems of the "lengthy step by step instructions were confusing them and they couldn't follow all of the re-directions to different instructions" along with the expectation that everyone work 60 hours a week at any hour of the day. When they excluded me for the 7 months, I was able to "Shorten the step by step instructions" which helped some people and later the Managers "Actually emailed out MY NOTES to everyone for the report generation instructions" which only benefited them while I was mocked and ridiculed over the entire 7-8 months from the time I was Hired. A person whom was out on leave returned and informed me of how the managers "unlawfully disclosed my disabilities to the entire department staff the next morning then lied to cover it up" and when I filed the 2nd complaint with Human Resources, the managers admitted to it because they knew of the witnesses. Still, throughout all that time, I was mocked, ridiculed, marginalized, harassed and excluded from the work tasks while others were provided pay raises and promoted. I know of 2 people whom were pulled aside and given raises on the spot back in January 2019 while I was excluded for my disabilities.

I would ask to schedule to meet with the primary manager Mng1, on multiple times in January 2019, February 2019 and March 2019 and on but he would outright IGNORE my request for a meeting to discuss issues. I scheduled it in his scheduler in February 2019 and on a slow snowy day(when we were both working in the same dept. & I could visually see him talking to friends), when “he was not doing anything but chit chatting with his buddies”, he cancelled my meeting request and repeatedly ignored my requests to meet with him. I have that documented over and over. There were 3 different people whom admitted to "Knowing of the mocking and ridicule and discrimination" from the investigations but would not give "specifics" for fear of their jobs and of course nothing was done.

Others were promoted and given raises while I was excluded, marginalized, ridiculed, harassed and mocked constantly. Then in the Summer 2019, when I was doing the payroll process, I was sabotaged in regards that I was given 3 payrolls and 2 were due on a Monday & Tuesday for submission. The larger one was on Tuesday, and both of these clients would not send in their PTO requests until the last minute. For example, Monday's would be sent in on Monday morning & afternoon, I would work on that and then the Tuesday payroll would start sending in stuff on Monday afternoon. Thus I would work Monday from say 8:45 am to 10:00 pm, then I would have to drive home and get up around 3:15 am in the morning to process the "Tuesday's PTO & pay items" for pay submission. I would have to record less hours on my time card than what I was actually working and what was actually "computer Logged in as actually working as". ABC Corp. did not want anyone to have overtime, frequently I would have to not record work hours worked at home because they didn't want people to have overtime. Mng1 would remove Holiday time for the week and a few weeks later, or next month or so, he would let me schedule a day off with regular holiday pay so I would not get the overtime from the actual work week. This went on during 2019 thru spring 2020. We had a meeting where we were “Threatened” by the fact that the “Contract with the clients” had an “Error Clause” that ABC Corp. would have to pay a fine of 15,000.00. Now I don’t know if that is true or not but management would intimidate the workers to work at all hours with not retention pay, one girl was actually pregnant in the hospital and had her
laptop and was entering Payroll entries to be submitted. Management thought that was “sooo very funny because when she was giving birth, she was sending in payroll!”

When I filed my second complaint in early June 2019, again I stated how I was being discriminated against, harassed, etc. etc. and during a meeting with HR, Mngr1 & his Manager, I asked “Why I was excluded for those 7 months, because I also informed them that it “WAS ILLEGAL” to Exclude me on the basis of my disability From 11/27/2018 through early June 2019, and Mngr1 & his manager responded that it was “because I was too slow”. There again I was “Excluded for a Time comparison of work tasks which was NEVER identified nor quantified!! I was excluded and retaliated due to my disability but I actually was NOT that muck slower!!! Your talking possibly “Fractions of seconds” thus ABC Corp. would use Artificial Intelligence as a “work task comparison against employees” but NEVER identified NOR allowed me as a worker “TO ACTUALLY SEE THE ACTUAL TIME COMPARISON USED AS THE BASIS OF THEIR DECISION”, “NOR ALLOWED ME TO RESPOND TO ANY SPECIFIC MATTER USED FOR ANY COMPARISON” to non-disabled workers, or Indian workers whom were NOT discriminated, nor retaliated against.

For the last bi-weekly week when I was doing the 3 payroll’s in late October 2019, after I complained about the long working hours, I actually worked over 120 hours in a 2 week period which should only have been for 80 hours. This was the end of September to early October 2019. The one employee was pregnant and was in the hospital and was “Actually giving BIRTH” and had her computer with her and "was submitting payroll at the same time as she was giving birth” and the same managers laughed and joked about her: “popping out a baby & popping out the payroll at the same time", this is how pathetic this company is. ABC Corp. favors foreign workers from India and from Guatemala and discriminates against domestic US workers for their benefit of “Outsourcing all the jobs to cheaper foreign workers, but they charge the US employers the US wages and keep the wage difference & fees for their profits. ABC Corp does not like anyone whom "Raises these issues" of contradictory training and discrimination by their management “whom is only following ABC Corp’s higher managements instruction. The majority of Higher management is of foreign Indian, ethnicity, thus they favor the workers of their same Indian ethnicity for preferred jobs and not domestic workers, for advanced training, and pay raises. I know of multiple people whom have worked there (US worker forced to transfer internally) for 6-8 years and have been held back and kept in the same lower paying job title while another worker whom came over because her Husband received an HB-1 work Visa during the Obama administration for programming was able to bring his wife & kids. The Wife also worked in the Payroll Department, and was promoted to specialist. She has been in the US less time that some of the other workers whom were age discriminated against for job advancement and pay raises. Indian worker whom is also from India and maintains a second home in India, was NOT selected for the collections job, where as the majority of the US domestic workers were Forced into the call center phone Collections job.

This also demonstrates the continued pattern of: Domestic US workers continued discrimination and direct sabotage of job training and advancement while ABC Corp prefers to keep and maintain their Indian workforce and outsourced Guatemalan workforce of over 200 + (as one trainer stated) wherever they are in foreign countries. ABC Corp systemically sabotages it's USA domestic workers so that they either Quit or are fired so they do not have to pay for “Outsourced retraining” as what is required under the law. This is also a systemic US domestic workers discrimination pattern of practice
which is also in violation of US worker’s civil rights. There are numerous court cases on how various Indian Outsourcing companies, whom continue to discriminate against US domestic workers.

The Payroll Job was completely OUTSOURCED to India employees around March 2020.

In late February 2020 – May 2020, I was DENIED a $3000.00 bonus for working through the end of the project because I would NOT sign a “employment discrimination General release from Liability” 3 page form. All of the NON-disabled workers were paid that $3000.00 bonus but I was NOT on the basis of my disability and not “Releasing ABC Corp from employment discrimination” on the document AFTER I had already complained multiple times and filed 2 complaints with ABC Corp’s Human Resources department. This is also discrimination on the basis of Disability because any “disabled worker whom is subjected to discrimination and complains about is and does NOT sign the general release form will NEVER get paid the bonus even though they did all of the work tasks.!!!

In early May 2020, I was FORCED into a “Call center Collections Job” which was in direct conflict with my disabilities. I have NEVER worked a “Call Center Job” where I would have to “Be on the PHONE HEADSET for the entire full shift”!! This is a direct health threat to my health as to my disability.

In late May 2020 I sent the new Head of Human Resources; an ADA accommodation request for this Collections job but again I was ignored just as I was in February 2019 by Mnger1.

I have never worked at any type of “call center environment” at all during my work history & I did not want to work any “call center job” with my disabilities. ABC Corp KNEW this but forced me into this Call center position, and ignored my inquiries about accommodations also. Their training was incomplete and practically daily something was not working over the cloud for the cloud access to account information. There were systemic problems like:

(A) The Training environment (not live menus) was NOT working and I did NOT have access for use for training. We were Forced directly into direct calls without hearing actual calls with actual customer complaints and situations. We could NOT access the menu’s WITHOUT a live customer which meant that we were unable to get familiar with the menus for adequate use.

(B) ABC Corp was negligent to only have one “SME” person (as they called them) to be available to ask operational questions for every 165 remote Cloud dial in “collection workers”. This would result in 10 – 15 minute delays for anyone to even respond to your text message questions in the “SME Chat Group”. There was 1- SME Chat Group for every day & the “Chats were also recorded”, so please, ask for some of those daily chat message files for your review! You will see how frequently “Incorrect training responses were provided back to the employee trainees from Texas and also in PA. There may have been some from other states, but I’m not sure.

(C) ABC Corp’s Trainers were frequently inexperienced with the work tasks and would instruct wrong and conflicting information on a specific order for a process to be done. The Trainer I had, named XXXXX, was a 19-20 year old kid from Guatemala whom said he was promoted after only working there for only 2 months to be a Trainer and he had never trained anyone before. This shows the “systemic discrimination towards US workers”.

445
(D) ABC Corps Management would also email out Wrong training instruction information also. For example: Their “Ops Manager: sent out an email to “314 trainee’s” with instruction to select from one dialer first while the second dialer would have a different classification to be selected and the Order instructed WAS WRONG & also to senior management, which instructed on a wrong process to disposition the calls.) which caused one call to be cross linked to a different person. Thus this would result in two calls being recorded wrong for the type of calls.

(E) ABC Corp’s Trainers did not train on how to determine the “Notes area” impacted various “promotional payment waivers” and how to properly get assistance from other departments for this. For example, Co. was offering a payment waiver for the people impacted by COVID-19. However the notes were confusing on how people recorded them and also how the automated computer system “Logged various activity”. These types of differences were not explained by the inexperienced trainers.

(F) ABC Corp’s trainers would instruct that there could be 2 late fee’s within a 12 month period which could be refunded as a courtesy credit to the customer however the trainers did NOT explain that the credit could only be input at a certain cycle period. My courtesy credit was working, then when I was switched, it did not work anymore and for about a month I called IT, and reported it to management but no one had any solutions. Plus the Trainers never explained that the system would only accept “one refund request” per cycle. This resulted in getting calls from pissed off customers whom were charged for 3 prior months late fees and the previous reps over the 3 months earlier did NOT correct the problem and the monthly late fees kept accumulating and then adding calculated interest on the late fees. We would be instructed to help to reverse the late fee’s but the system would not accept the second one then we would ask questions to the SME chat and the SME rep most of the time would not respond with the proper information to solve the issue. This would result in the customer getting an additional month late fee with interest and then the customer was just pissed off and wanted the account closed. Well this is not my fault because “Why didn’t the prior Collection Rep (presumably from Guatemala) from the 2-3 months earlier correctly fix the customer’s problem?” This was a common occurrence with these pissed off customers. Customer’s would not have the issue resolved for months, way long before I even started being trained to take calls.

(G) 8/29/20 Sat - Ph # from Texas. to say that: 90 employees were being pulled off the dialer because: some of the training material was wrong and people had to be re-trained. This also shows negligent training on the part of ABC Corp and it’s selected trainers. If people are informed wrong and contradictory training information, then obviously something will be wrong.

(H) ABC Corp’s Trainers also provided wrong instruction on the account labeling of a Joint account owner. We were informed that a joint owner would be listed as a secondary on the account when this actually was NOT the case. A second name could be on the account and ALSO could NOT have account ownership to the account. This was not properly explained either which would cause contradictory issues.

(I) ABC Corp’s cloud system would frequently lock a person out of the cloud website after a person went to lunch and then could not login. Thus a person would have to call the IT department and wait for assistance for the profile to be reset to be able to login.
(J) ABC Corp’s system would constantly be “delayed” from when an “auto-dialer to a customer would be automated but there would be a “long delay from when any customer account information would show up from the two dialer systems”. This would cause a customer answering and saying: “what do you want? You dialed me!” and you don’t even get any information on the customer name or state they live in to be able to respond properly. Then the customer would hang up.

(K) The equipment hardware also had problems. My mute button on the headset also broke and the headset could not be used to take any calls. (Locked in the Mute mode)

These are just a few of the many, many more issues, which were a constant problem and issue. When I would:  “Recognize these issues” and bring them up in both emails and in the chat groups or Zoom sessions, then ALL of the additional people in the group would ALSO agree about how we are being provided wrong information for the training and others would then also complain about the Improper training that they also received.

ABC Corp and their management did not like the fact that I could “Identify directly specific issues which were wrong” and retaliated against me for stating the truth.

Just to speed things up a bit, (I could go on and on about additional specifics) to return back to the historical systemic discrimination that I have experienced from working at ABC Corp.

In November 2019 thru February 2020, the managers individually traveled to India to Train the new Indian employees based in India to do all of the payroll processing since it would be completely be 100% outsourced to India. In February 2020 and early March 2020 we assisted with the training and outsourcing to the Indian employees. Then in mid March 2020 the COVID-19 pandemic occurred. We were sent home due to Pennsylvania’s state closure to early June 2020. In August on 2019, when a lot of employees were quitting, ABC Corp had a Bonus for the employees whom stayed to complete the payroll to the outsourcing to India in Feb/Mar 2020. In May 2020, all of the employee’s were paid their Bonus, but to receive the bonus, they had to sign off on a: “ 3 page LEGAL RELEASE from any form of discrimination etc.”. This 3 page Legal Release is also unlawful because any disabled person whom complains of discrimination and does not sign it will NEVER be able to be paid a bonus, which also is unlawfully based on their disability. I refused to sign the 3 page Legal Release and I was NOT paid the $3,000.00 bonus that ALL the NON-disabled employees were paid. I can provide you documentation on this also. From mid-march to May, we were supposed to “apply to new jobs”, however we were told that we could NOT apply to different jobs in a different “category” however later I learned that ABC Corp would “select Guatemalan employee’s age 19-20 Yrs old to be Trainers” and they didn’t Apply to these promoted jobs. All ABC Corp. cares about is to outsource US Jobs to Indian and other foreign lower paid workers for the wage profits for them to keep the wage difference of what the charge the US business client. Employees at the client were laid off by its client due to the Payroll outsourcing. This is systemic and ABC Corp seeks out major US employers to streamline various processes for keeping the spread on the wages of lower paid workers for profits. I applied to a different job, one NOT requiring any call center, NOR headset use, however I was not selected. I should have been laid off due to the outsourcing and I would have been able to get state retraining however ABC corp FORCED me into a Call center Collections Job that I didn’t want and I told them I didn’t want it.
I started the FMLA on 8/27/20 and used most of the time off after that for care and while I was in the process of getting the FMLA paperwork, again I asked about ADA accommodations which were ignored by HR. On August 27 & Aug 28, 2020 again the FMLA and Accommodations were brought up in emails sent to Human Resources in PA. Copies of the emails are included & the accommodation papers which NEVER HAD THE JOB DESCRIPTION SENT FOR THE WORK TASKS, nor did ABC Corp identify what grading criteria would be used for calls which were already putting me in harm’s way with my disabilities, that they had Knowledge of.

ABC Corp. also allowed non-disabled workers to participate in programming training over a 6 month time period while they excluded disabled workers from participating and did not allow for accommodations for the participation of programming training from around May 2020 thru late September 2020.

As for ABC Corp’s “Reason’s for termination = “Low quality scores”; they NEVER HAD ANYONE FROM MANAGEMENT PROVIDE ANY INFORMATION ABOUT LOW QUALITY SCORES AND NEVER RESPONDED FOR MONTHS REGARDING INQUIRY ON “5/28/20 EMAIL” FOR HOW ASSESSMENTS ARE DONE.

Specifics can’t be asked when it is never provided. Plus I NEVER requested to be put in this job position, it was a direct retaliatory action applied to disabled worker when Indian staff were NOT put in the same job.

ABC Corp NEVER Provided a Job Description for the Collections Job.

ABC Corp Never Identified “What Criteria would be used for grading or evaluating work tasks” and most of the training was FLAWED with incorrect information provided or wrong training processes
instructed or NO proper instructions. Plus NO access to website system for Practice and NO training for already angry existing customers due to their own foreign existing staff with wrong call handling.

ABC Corp. does NOT evaluate the same disabled workers and also the US domestic workers with the same grading criteria as it does with their Foreign Indian or Guatemalan workers and management staff.

At no time was any calls reviewed with me nor discussed by any manager. At no time were any type of quota type standard discussed with me either. Since I had invoked again both the FMLA and ADA accommodations about the negligent training and retaliation, I was helping to care for my family member and was in the process of getting the appropriate doctors (two different ones for each form) to complete the FMLA and the ADA paperwork. Both Doctors have been very busy with all the setbacks due to the COVID-19 pandemic. Under the Law, you have 15 days plus an additional 7 days to get the FMLA paperwork back and I had emailed them a letter from the one doctor whom was working on the paperwork. ABC Corp. sent an email on Thursday 9/10/20 at 8:03 pm in the evening, that I didn’t see until later stating that: “Pursuant to out telephone call on 9/10/2020 (only a short 20 second voice mail message not received until later), ABC Corp is terminating your employment as of 9/10/20, based in part, on multiple performance issues.” And that is all that is stated. Nothing was discussed as a problem nor reviewed and It is also retaliatory conduct in a continued pattern of practice which will be easy to demonstrate this treatment towards me versus non-disabled workers.

ABC Corp Retaliated against me for my disabilities and for my requests of FMLA & ADA and identification of their own negligent training which was systemic and also impacted probably hundreds of other US workers, and they didn’t like the fact I was Identifying how their own trainers and manager’s were instructing us with WRONG INFORMATION, which the entire employee group also agreed upon, and will show within the “chat meetings” and recorded meetings Prior to the termination.

ABC Corp continuously ignores and avoids the matter and continues to discriminate and retaliate against its workers and disabled workers. All you have to do is look on Indeed’s “Employee comments” from many workers, and they complain about these same matters or issues that I have mentioned but since they check their “Indeed Reputation” online, they have “counter positive manipulation comments” to post also, as this is a standard process with “AI monitoring” and comment manipulation which is done online. (One star & 5 stars, gives an average of 3 stars online, to manipulate the true nature of the work environment.)

Thus to wrap up a long story short, I have been discriminated, harassed and retaliated against for my disabilities, and for my complaints of the discrimination, harassment and retaliation which has been systemic by this company and charges will be filed

Thank You
General Comment

Computers don't understand the unique needs of individual people, nor accommodate their unique needs.
I'm not a server, but as a patron I would be very unhappy if I knew my server, and therefore me, was being monitored. Please do not allow this technology.
**PUBLIC SUBMISSION**

**Docket:** OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

**Comment On:** OSTP-TECH-2023-0004-0001
Request for Information: Automated Worker Surveillance and Management

**Document:** OSTP-TECH-2023-0004-DRAFT-0171
Comment on FR Doc # 2023-09353

---

**Submitter Information**

**Name:** Anonymous Anonymous

---

**General Comment**

Testing for extension
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0001
Request for Information: Automated Worker Surveillance and Management

Document: OSTP TECH 2023 0004 DRAFT 0172
Comment on FR Doc # 2023-09353

Submitter Information

Email: [REDACTED]
Organization: Retail, Wholesale and Department Store Union (RWDSU/UFCW)

General Comment

Amazon employs an estimated 1.3 million people around the world, of whom 950,000 work in the U.S., within a workforce that experiences 150% labor turnover per year. Amazon prides itself on its development of an internal technology infrastructure that moves products quickly from click to consumer. This infrastructure allows Amazon to direct every aspect of picking, packing, and preparing orders for shipment through dystopian worker surveillance techniques, from ID-tagged wristbands and item scanners to navigation software and thermal cameras that track worker movements. But Amazon’s use of technology extends beyond the factory floor to requiring workers to download Amazon’s app on their personal devices, predominately through smartphones, but also tablets and wearable devices. In many cases, personal electronic devices used by workers are also shared by multiple members of their families.

Amazon has various employee apps purportedly to help workers “manage their work life at Amazon.” Though Amazon claims that use of the AtoZ App is voluntary, the need to download the AtoZ app is essential for working at its fulfillment centers. The App is one of the few places where workers can check schedules, claim overtime, claim extra shifts, get paystubs, and request time off. The App may be the only place where a worker can find their supervisor’s name in a workplace where many never meet a manager. During worker orientation, supervisors and coworkers direct new warehouse employees to install the Amazon’s AtoZ app on their own personal electronic devices.

The Amazon AtoZ app was developed by Amazon Mobile LLC. The App covers the majority of Amazon’s U.S. logistics network. This app when downloaded to workers’ personal devices has access to their
• Location (approx. location and GPS)
• Photos/Media/Files
• Storage
• Camera
• Microphone
• Wi-Fi connection information

453
• Other functions to be discovered with App credentials

Data collected by the use of the App may be shared with other companies and cannot be deleted. Workers need to have credentials, specifically active employment, to gain active access to the App.

In October 2020, internal confidential Amazon documents were leaked describing a new technology system called geospatial Operating Console (SPOC) to help Amazon analyze and visualize at least around 40 different data sets, among them, many related to helping Amazon gain indications if workers are mobilizing and union organizing at its facilities.

This system and similar technological systems developed by Amazon, the second largest private sector employer in the US, is troubling, particularly with policies and regulations lagging behind how worker privacy information can be collected and used.

In conversations with technology experts in the field, there has yet no independent assessment that has been conducted that gives any transparency or understanding on what data the AtoZ app collects from workers, when data is collected (during working hours and/or outside working hours), how data harvested by the app is used, if the end user experience justifies the data collected by the App, if information collected by the App is being sold beyond its primary stated usage.

The Apps access to workers personal devices’ GPS, camera, microphone and wi-fi connection information, along with the lack of legal regulations and lack of information on how data that is harvested from workers raises fundamental questions to the ability for workers to exercise freedom of association, speech and assembly working at Amazon. With stringent intellectual tech policies protecting companies like Amazon, any independent inquiry into these questions without explicit permission from the company is impossible. Equally protective and stringent policies and regulations are required to protect end users, in this case, workers is necessary to protect against inappropriate use and abuse of data that violate workers’ rights, civil rights and human rights. The issue of usage of these types of apps are expanding as Amazon sells similar labor-management types apps to private businesses and competitors bring online competing apps and tools.
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0173
Comment on FR Doc # 2023 12995

Submitter Information

Email: [Redacted]
Organization: Data & Society Research Institute

General Comment

See attached comment.

Attachments

Attachment 1_Data and Society_OSTP_Comment_June2023_Final-1
June 21, 2023

Response to the White House Office of Science and Technology Policy’s Request for Information on Automated Worker Surveillance and Management

Data & Society Research Institute submits this comment in response to the Request for Information (RFI) on Automated Worker Surveillance and Management published by the White House Office of Science and Technology Policy (OSTP) on May 1, 2023. Data & Society is an independent, nonprofit research institute studying the social implications of data-centric technologies, automation, and artificial intelligence. We produce empirical research that challenges the power asymmetries created and amplified by technology in society.

Automated worker surveillance and management systems present grave risks to workers, their families, and their communities. Many employers are using such systems in unlawful ways that undermine workers’ health, safety, pay, autonomy, legal rights, and collective power.

Informed by empirical research and worker interviews conducted by Data & Society, this comment describes practices of automated worker surveillance and management, including how they operate and how pervasive they are (Section I) and how they are harming workers and their rights (Section II). We then offer policy recommendations for the Biden-Harris Administration to address the harms of these systems under existing federal law (Section III).

As the White House seeks to advance equity and worker voice in federal technology policy — as embodied in its Blueprint for an AI Bill of Rights¹ and Executive Order 14091² — executive agencies must act swiftly to redress the harms resulting from automated worker surveillance and management. Data & Society encourages the Office of Science and Technology Policy, Domestic Policy Counsel, and Office of Management and Budget to coordinate a comprehensive approach to protect workers from invasive and unlawful employer practices.
I. Worker surveillance and algorithmic management are independent employer practices that undermine worker power and degrade standards of work.

Although in this comment we generally adopt the RFI’s use of the term “automated worker surveillance and management,” we offer a clarification at the outset: the practices of worker surveillance and algorithmic management are discrete employer practices and should be understood as such. Worker surveillance harms workers even where supervision is performed by human managers, not by automated systems. And algorithmic management harms workers even where workers are remotely managed through external data like traffic and weather patterns or customer demand. Addressing the two practices as a unified system — as one closed circuit of worker data feeding into automated systems that thereafter generate employer decisions — elides other harms resulting from automated worker surveillance and management.

In retail, for instance, employers use automated scheduling technologies that incorporate data on customer shopping patterns (collected from surveillance of customers) and weather conditions to determine staffing and scheduling, which has exacerbated precarity, stress, and economic instability for low-wage workers and their families.3 Many service jobs also use customer ratings and reviews in management decision-making, including determining workshifts, disciplining employees, and termination.

Addressing technology-mediated harms to workers will require looking beyond direct monitoring of workers to employers’ broader deployment of data practices and automation. Restricting or eliminating the collection of workers’ personal data will not end the harms of algorithmic management, which can continue based on other sources like customer reviews, weather and traffic data, or seasonal retail patterns.

Although workplace surveillance is not a new practice, it is rapidly expanding to impact new sectors and more workers in more invasive ways.

Worker surveillance has operated in the workplace for centuries. While some trace the first instances of scientific management to Frederick Winslow Taylor’s management principles around the early twentieth century, the measurement of human laborers and productivity can be seen in the record keeping of enslaved Africans centuries before the first factories were built in England.4 The word “surveillance” itself — deriving from older words like “survey” or “supervise” that did not quite capture the new practice of employers gaining informational advantages over workers — emerged around the creation of modern capitalism.5
Managers have long collected information on workers to analyze their skills, productivity, and fitness for employment, as well as to make predictions about worker behavior. If there is a difference now, it is that technical advancements have made worker surveillance and data collection nearly constant and extremely detailed. Today’s invasive, continuous, and opaque surveillance systems descend from a long history of employer practices to wrest control from workers — from early paper filing systems and statistical analysis to today’s automated data collection and decision-making.6

As many workplaces no longer are confined to centralized physical locations, bosses are implementing new technologies to monitor dispersed and asynchronous workforces. The app-based, platform, or “gig” economy in particular has introduced a new frontier of worker monitoring. Employers like Uber, DoorDash, and Amazon remotely monitor their “independent contractors” by requiring them to use apps with geolocation, checklisting, and photo functions. This permits app-based employers to oversee a decentralized workforce, directing where workers go, setting pace standards, and even remotely geofencing or restricting areas of work. Some employers also use new domains of surveillance like internet-connected doorbell cameras. For instance, through its popular Ring-branded doorbell cameras, Amazon has created an ecosystem in which customers monitor and instruct delivery workers.7 Even as “independent contractors,” this workforce faces hyper-surveillance on two fronts: through the extensive geolocation and task monitoring on Amazon’s app and through the doorbell cameras watching customers’ front doorsteps.

Surveillance is most prevalent in low-wage industries where managers can easily measure and quantify workers’ tasks.8 But increasingly, some employers are extending surveillance to jobs where work is not as easily quantifiable. In white-collar jobs, surveillance may look like keystroke and mouse monitoring, productivity scores, and photo requirements.9 Since the COVID-19 pandemic, as more workers began working from home, employers have been applying such surveillance to workers’ home activity. Because these tools do not account for work that cannot be easily quantified, such as ideation or contemplation, workers feel pressure to perform to metrics rather than their job responsibilities.10

By automating worker decisions on a massive scale, algorithmic management permits new forms of employer control.

Whereas the surveillance of workers by their bosses dates back at least centuries, automated management systems are a genuinely modern invention. Because the practice is novel — and because its meaning thus may be contested among different parties — we situate the practice as one of control, on a massive scale:
Algorithmic management is a diverse set of technological tools and techniques that structure the conditions of work and remotely manage workforces. Algorithmic management systems’ emergence in the workplace is marked by a departure from earlier management structures that more strongly rely on human supervisors to direct workers. Algorithmic management enables the scaling of operations by, for instance, coordinating the activities of large, disaggregated workforces or using data to optimize for desired outcomes like lower labor costs.\textsuperscript{11}

For now, algorithmic management is most visible in app-based or on-demand labor to manage, discipline, and terminate app-based workers who nominally are hired as independent contractors.\textsuperscript{12} App-based employers such as Uber, DoorDash, and Instacart use algorithmic management to nudge specific worker behavior; this includes directing workers to locations and incentivizing particular schedules.\textsuperscript{13}

Beyond app-based jobs, employers use automated worker management in some fashion in many occupations, especially among low-wage work, such as hospitality, retail, logistics, warehousing, agriculture, hospitality, domestic work, and healthcare. Because tasks in these industries are easily measurable, they are susceptible to datafication. When tasks are susceptible to datafication, many employers seek to lower labor costs and increase profits by managing workers through automated systems. The workers who labor under this robotic supervision are often immigrants, women, and people of color who have historically faced a more exacting degree of monitoring.\textsuperscript{17}
In this section, we will document harms that automated worker surveillance and management systems inflict on workers in four categories:

1. Working conditions plummet, characterized by work intensification, unpredictable pay, and the erosion of worker autonomy. As employers use automated worker surveillance and management systems to watch, atomize, supervise, and discipline workers, workers’ satisfaction and job quality plummet. Pervasive surveillance and automated micromanagement make human beings feel like robots. Without much-needed policy action — whether sectoral regulation, data minimization, or outright prohibition — these systems trample on the basic dignity in work.

The heightened speed and efficiency pressures enabled by automated systems can lead to increasingly unsafe and precarious workplaces, both by exacerbating physical and mental health risks and by undermining labor rights and protections. Research by the University of California-Berkeley Labor Center has documented higher rates of warehouse injury in more automated warehouses. At Amazon warehouses, punishing data-driven quota systems have led to injury rates far exceeding the industry average. Some states, including New York and California, have passed legislation to set quota limits, and have placed bans on firing warehouse workers for missing quotas that interfere with bathroom and rest breaks.

Algorithmic systems also disrupt work quality by undermining wage predictability. Because app-based employers need to scale worker availability to customer demand — while at the same time invisibilizing their own means of control over “independent contractors” — companies like Uber do not directly order workers to go somewhere but instead use wage manipulators to shift worker behavior. Such wage manipulators, which may lead to variable and unpredictable wages among workers, may appear as bonuses available only to workers who meet certain metrics, “surge” pay that later disappears, or incentives to keep workers on the app. Drivers for Uber have reported deep dissatisfaction with their employer’s digital trickery. While these systems of algorithmic pay manipulation are most prevalent in the delivery and transportation sectors, they may spread as more industries seek to “gig out” their workforce to lower labor costs.
Pervasive automated surveillance and management can erode the basic human dignity in work. Care workers’ experience with Electronic Visit Verification (EVV), a tracking app mandated as part of Medicaid fraud oversight in paid personal care and home health care, offers an instructive example. While EVV systems must be “minimally burdensome,” per statutory requirements, our research found that they place significant challenges on both workers and public benefits recipients. Minor missteps in worker compliance often lead to delayed or lost wages, and requirements that workers log their activity in real-time or within geofenced zones (enabled by GPS tracking) make it more difficult for workers to provide care. Workers interviewed by Data & Society reported that the new surveillance practices have a criminalizing effect, making them feel like they are under suspicion of the state, while also making workers comply with onerous productivity metrics. Like other industries characterized by high surveillance and automated decision systems, the homecare industry is a workforce comprised primarily of women — particularly immigrants and women of color — where low wages and difficult-to-enforce labor protections have generated high turnover and labor shortages despite soaring demand. Labor and disability advocates have warned that punitive digital surveillance practices like EVV are having a chilling effect, weakening the US care infrastructure.

2. Algorithmic management allows employers to unlawfully create the illusion of worker independence to disposess workers of their rights. Like the offshoring strategy employed by big corporations around the mid-twentieth century to access cheap labor abroad, many employers now use technologies like automated worker surveillance and management to “fissure” traditional employment to lower labor costs. Because most state and federal worker protections apply only to workers classified as employees, and not to independent contractors, companies have an incentive to reduce their obligations by insisting that their workers work at their own discretion and not under the supervision of a boss.
By labeling their workers as “independent contractors,” many companies deprive workers of core rights and protections such as the right to a minimum wage, overtime pay, collective bargaining, unemployment compensation, and protection in the event of a disability. This illegal practice existed well before modern technologies, but algorithmic management has supercharged it.

By making it much easier to create the illusion that workers control their own working conditions, algorithmic management enables companies to benefit from the artifice of worker flexibility while maintaining control over when, where, and how “independent contractors” do their work. Put another way, employers are using technology to superficially distance themselves from their workers — bolstering the rights-denying claim that their workers are not employees — even as the overall business structure remains one of top-down control.

Beyond app-based transportation and food delivery workers, employers’ use of automated management technology has spread in recent years. Retail and e-commerce have rapidly shifted to an independent contractor model, with major retailers like Amazon hiring scores of on-demand delivery workers through Amazon Flex (described in Section I). Other employers, like Target and Walmart, are mimicking this model, expanding the workforce of app-based delivery drivers. Increasingly, grocery stores are laying off full-time delivery employees and replacing them with Instacart workers. The healthcare industry too has seen experiments to classify nurses, dental hygienists, occupational therapists, and other healthcare workers who work through an app as independent contractors.

3. Opaque automated systems make it harder for workers to speak up. Black box algorithms obscure the precise mechanisms of data collection, analysis, and decision-making, exacerbating power imbalances between workers and bosses. This opacity allows employers to leverage even greater control over workers. With little information about how decisions are made, workers have less power to speak up for themselves, challenge decisions, and identify systemic harms in order to take collective action.

For example, in a 2021 settlement with the Federal Trade Commission, Amazon agreed to pay $61 million back to Flex drivers for automated tip theft between 2016 and 2019. Through interviews with Flex drivers, Data & Society researchers observed that the Flex app helped to obfuscate, and likely prolong, Amazon’s tip theft activity. The Flex app did not provide drivers with a breakdown of their pay and offered no pathways for disputing a payment.
Transparency also came to the fore during the COVID-19 pandemic, as employers began to implement or repurpose technology to monitor worker health. As detailed in Data & Society’s report, *Essentially Unprotected: Health Data and Surveillance of Essential Workers During the COVID-19 Pandemic*, worker health data collection occurred mostly in a haphazard way and mostly for the benefit of the employer. For example, Amazon used the pandemic as an opportunity to expand its regime of worker monitoring, repurposing technology like cameras and introducing new tools like its “distance assistant.” Workers interviewed by Data & Society did not understand how this data was used, if at all, for the improvement of their health and safety. In many cases, employers did not share information on infections in the workplace, which was critical for workers to understand how to protect themselves from COVID. This lack of transparency not only eroded trust between employers and employees, but it resulted in increased infections and anxieties about workplace safety.

4. Automated worker management systems permit employers to avoid their nondiscrimination obligations. Many employers are using algorithmic management systems to outsource worker monitoring and discipline, incorporating customer reviews as data on worker performance. Research indicates, however, that customer reviews can lead to discriminatory outcomes, with women and racialized minorities receiving poorer reviews on average. Workers thus face potentially biased, discriminatory assessments by customers, which can lead to unlawful discipline or firing.
Case study: Discrimination in Delivery Work

Our recent report At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers details how employers like Amazon incorporate customer evaluation into automated delivery worker management. Similar to Uber driver ratings, Amazon Flex workers must maintain an acceptable “standing” that is calculated based on factors such as on-time delivery and customer reviews. Amazon then awards points to workers with high standings, which can unlock “Flex Rewards” such as preferred scheduling priority. Conversely, low standing can place drivers at risk of deactivation. Because customer ratings and reviews make up a substantial portion of a driver’s standing, a Flex delivery worker faces discipline and potential termination based on subjective customer opinions.

Our research on delivery work and outsourced customer reviews frequently surfaced workers’ concerns about bias and discrimination — and their perception of otherness, generally. Compared to white delivery drivers, drivers of color interviewed by Data & Society spoke more reflectively and at greater length about their experiences of being watched during their work. They were acutely aware of their presence in someone else’s neighborhood, often noting that in predominantly white communities they felt they were being monitored by residents.

Modern technologies thus have enabled a new employer-consumer regime of worker surveillance. Amazon misclassifies their Flex workers as contractors because algorithmic management creates an illusion of worker independence. As contractors, Flex delivery workers cannot access federal antidiscrimination protections. At the same time, Amazon has leveraged its consumer technologies, like Ring doorbell cameras, to incentivize customers to monitor, instruct, and critique the workers delivering goods to their home. At the intersection of consumer surveillance and automated worker management, Flex workers face acute risks of bias and discrimination in a work structure where workers have no legal recourse if they are disciplined or fired due to bias or discrimination.
III. Policy recommendations

While existing federal laws may not capture all the harms of automated decision systems, those laws are nevertheless broad and suffice to address many of the harms workers are currently experiencing from such systems. Accordingly, federal agencies should use their existing statutory authority to address the harms of these systems through proactive guidance and targeted enforcement.

Restoring employee rights

It is not just that employers are using automated surveillance and management technologies in ways that violate workers’ rights. It is that many employers are using such technologies to conceal their control over workers and to deny that workers have employment and labor rights in the first place.

To begin to restore workers’ access to statutory rights, there must be clearly defined employment relationships that set out workers’ broad access to rights, especially in the face of automated surveillance and management tools. The Department of Labor’s (DOL) proposed rule on independent contractor classification under the Fair Labor Standards Act is a good start to ensuring that workers who are building the business of another can access minimum wage and overtime protections. Notably, in clarifying the Department’s return to the six-factor economic realities test, the rule proposes to assess an employer’s control by, among other things, expressly considering their use of electronic management technology. The DOL should retain that guidance in its final published rule.

In a similar fashion, the National Labor Relations Board’s (NLRB) rulemaking to restore “joint employer” accountability under the National Labor Relations Act (NLRA) should address the role of technology in preventing or chilling worker organizing. Unlike the DOL’s independent contractor rule, the NLRB’s joint employer rulemaking does not explicitly address an employer’s use of surveillance. The NLRB should strengthen its proposed rule by clarifying in the final rule that employers’ use of automated surveillance and management technology is presumptive indicia of an employer’s “authority to control” or their direct or indirect “power to control” under the NLRA.

Wage and hour protections

Even if properly classified as statutory employees, workers face the punishing demands and degraded working conditions of automated worker surveillance and management. These modern technologies present certain challenges to existing worker protection statutes — beyond the threshold problem of classification — that agencies should resolve through guidance. Key among those challenges is the issue of compensable time under automated management systems.
After publishing its final independent contractor rule, the Department of Labor should prioritize the issue of compensable time for workers laboring under algorithmic management systems. Many such systems, particularly those that make up the app-based business model for companies like Uber and DoorDash, start from the premise that workers are not paid for all the time they are on the app. (Hence: app-based companies’ behavior incentives that lead to individualized and unpredictable pay rates, as described in Section II). Further, because algorithmic systems often do not show how take-home pay is calculated, many workers do not know that a significant amount of their work is unpaid. Clarifying the legal boundaries of compensable time is a necessary step to protecting app-based workers’ financial security.

Generally, there are three categories of time spent working for app-based companies: “P1” time, when workers have the app open and are waiting for a job; “P2” time, when workers have accepted a job and are en route to pickup; and “P3” time, when workers are performing the job itself, e.g. transporting customers inside the vehicle. App-based employers do not pay for workers’ P1 time (or associated expenses).

Even if classified as employees with statutory protections, app-based workers’ pay may not reflect fair compensation for their labor if companies continue to reject paying workers for P1 time. Companies may continue to commit wage theft by calculating only workers’ P2 and P3 time.

To redress the harms that these systems are creating, the DOL’s Wage and Hour Division should put forward guidance on how it assesses compensable time for workers whose pay is set, and whose work opportunities are structured, by automated management systems. Specifically, it should address whether app-based workers’ time waiting for a job on the app (P1 time) constitutes time that workers are “engaged to wait.”

Health and safety
Due to the extensive evidence of bodily injuries and musculoskeletal disorders resulting from automated surveillance and management systems, as well as the mental health risks and stresses, the Occupational Safety and Health Administration (OSHA) should incorporate these employer practices into its sector-by-sector guidance on workplace injury prevention and through new guidance to identify workplace injury risks and solutions in warehousing. Further, the National Institute for Occupational Safety and Health should fund new research into the effects of automated surveillance and management systems on workers’ physical and mental health. Finally, OSHA needs much more funding to investigate employers’ infractions of health and safety regulations. It should also consider alternative mechanisms of monitoring and enforcement. Co-enforcement models at the local level, where worker-led councils conduct peer-to-peer education to identify health violations, have shown promise in making worksites safer. In Los Angeles County, for example, public health councils have centered the health needs of workers to more effectively monitor workplace safety.
We also encourage the Biden-Harris Administration to place health and safety issues within the broader practice of biometric data collection. Employers are increasingly collecting workers’ biometric data, such as fingerprints, iris recognition, retina scan, heart rate, and step counts, for the ostensible purpose of monitoring workplace safety.49 But as we document in Essentially Unprotected, described in Section II, it is unclear — especially to the workers being surveilled — whether the collected data is in fact being used for the purposes of workplace health and safety. Some employers may be invoking “health and safety” to ramp up invasive, near-constant worker surveillance that they may use for other purposes later, such as to feed into automated management practices. Regulators and policymakers should pay attention to biometrics as a new realm of workplace surveillance and management.

Employment discrimination

Given the potential for bias in hiring, promoting, and firing, we were pleased to see the Equal Employment Opportunity Commission’s (EEOC) recent Title VII guidance focusing on algorithmic practices in selection procedures.50 This is a positive step for the Commission to educate employers and software vendors about how their use of automated technologies can violate civil rights laws and offer advice about the steps necessary to come into compliance.

We note that the EEOC’s guidance includes as examples “automatic resume-screening software, hiring software, chatbot software for hiring and workflow, video interviewing software, analytics software, employee monitoring software, and worker management software.” We encourage the EEOC, as well as the Administration more broadly, to additionally consider the employer practice of offloading worker assessments to customers. By transferring worker evaluations to customers, many companies are placing their workers at risk of discriminatory and biased assessments, which could lead to their discipline and termination. Similar to the Commission’s recent guidance that employers are still responsible for algorithmic tools designed or administered by a third-party software vendor, employers should not be able to escape their nondiscrimination obligations by outsourcing worker assessments to customers.

Worker organizing

Modern surveillance practices are so thorough, minute, and near-constant that they are chilling workers’ protected right to collective activity.51 For that reason, we were encouraged to see NLRB General Counsel Abruzzo’s October 2022 memorandum on worker surveillance, in which she proposed a framework for “the Board to find that an employer has presumptively violated Section 8(a)(1) where the employer’s surveillance and management practices, viewed as a whole, would tend to interfere with or prevent a reasonable employee from engaging in activity protected by the [NLRA].”52

The NLRB should act swiftly to adopt the general counsel’s proposed framework to address the chilling effect that modern surveillance and management practices are having on workers’ protected right to organize.
Public sector adoption of automated worker technologies

Public institutions, starting with the US government, have the power to entrench or reject the technocratic ideologies that underpin automated worker management and surveillance systems. Even now, the federal government deploys these technologies in federally-funded programs. But it has the opportunity to course-correct and set norms of decent work quality that limit or prohibit anti-worker automated systems.

The government’s adoption of EVV in Medicaid, for example, accepts the premise that fears of criminality and fraud in services for poor people warrant demeaning surveillance. It moreover accepts the premise that technology can solve social problems like a crumbling care infrastructure. But the evidence shows that EVV’s invasive surveillance practices are hurting the delivery of federally-funded care services. Workers are leaving the industry due to EVV’s onerous burdens, despite the Administration’s stated commitment to increasing access to care and supporting caregivers.

EVV is only one example. We urge the Administration to consider not only whether and how the government procures and deploys automated worker technologies, but how it may, as the foremost public institution of the United States, disrupt the technocratic logic driving new domains of worker exploitation.

Conclusion

Data & Society encourages OSTP and the Biden-Harris Administration broadly to coordinate efforts across the federal government to protect workers from invasive, degrading, and unlawful automated worker surveillance and management technologies.

Respectfully submitted,

Brian J. Chen, Policy Director
Livia Garofalo, Researcher, Health & Data / Trustworthy Infrastructures
Alexandra Mateescu, Researcher, Labor Futures
Aiha Nguyen, Program Director, Labor Futures
Eve Zelickson, Researcher, Labor Futures
Endnotes


5 Josh Lauer and Kenneth Lipartito (eds.), Surveillance Capitalism in America 4 (Univ. of Pennsylvania Press 2021) (dating the word’s etymological origin to Europe’s transition “from the ancien regime of subjects under a king in a seigneurial economy to citizens of a state in an economy of private property”).

6 Id. at 2, 9.


8 Nguyen, supra note 4, at 4.


10 Id.


Response to the White House OSTP’s Request for Information on Automated Worker Surveillance and Management


16 Mateescu and Nguyen, supra note 11, at 4.


18 See generally Nguyen, supra note 4.


23 Id.

24 Id. at 33 – 42.

Response to the White House OSTP’s Request for Information on Automated Worker Surveillance and Management


27 *Id.*


39 Nguyen and Zelickson, supra note 7.

40 Id. at 20 – 21.

41 See, e.g., Weil, supra note 28; Nguyen, supra note 4; Callaci, supra note 30 (detailing the use of electronic monitoring in franchising as employers seek to avoid employment and labor law compliance).


43 Id. at 62250 (“Control may be exercised through nontraditional means such as automated systems that monitor performance, but it can be found to be control nonetheless.”).


47 Id.


53 Mateescu, supra note 26.

PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0174
Comment on FR Doc # 2023 12995

Submitter Information

Email: [redacted]
Organization: HR Policy Association

General Comment

See attached file(s)

Attachments

HRPA Comments OSTP RFI June 2023 FINAL
June 28, 2023

Mr. Alan Mislove  
Assistant Director for Data and Democracy  
Office of Science and Technology Policy  
Washington, DC 20500

RE: Request for Information: Automated Worker Surveillance and Management  
(88 FR 27932; Document ID OSTP-TECH-2023-0004-0001)

Dear Mr. Mislove:

HR Policy Association submits these comments in response to the request for information (RFI) from the White House Office of Science and Technology Policy (OSTP), regarding the use of automated tools in the workplace.¹

HR Policy Association is the lead public policy association of chief human resource officers (CHROs) representing nearly 400 of the largest employers doing business in the United States and globally. Our member companies employ more than 10 million individuals in the United States and are committed to maintaining a culture of trust in the workplace, especially as it relates to workforce data. Our organization and our members provide a unique perspective on the current and future role of automation in the workplace and the potential of automated systems, including those using artificial intelligence (AI) to assist companies in making employment decisions and communicating with their workforce.

The swift growth of automation technology raises substantial questions about how laws and regulations can promote the advancement of trustworthy AI technology and maximize its benefits while mitigating risks. Association members are committed to using technology in the workplace in a transparent and nondiscriminatory fashion. It is imperative, therefore, that prior to making consequential regulatory decisions about the use of automated systems in the workplace, policymakers engage regulated entities and other stakeholders to ensure that any future decisions are based upon the most current, accurate information possible about the current and anticipated state of AI technology and its societal implications.

The Request focuses specifically on the use of automated tools by employers to “surveil, monitor, evaluate, and manage” workers. While the Request acknowledges that automation may be used for a wide range of purposes in the workplace, it focuses on those tools which “pose risks to workers and may even violate labor and employment laws.”

HR Policy Association members do not condone unreasonable and intrusive surveillance that serves no business purpose and does nothing to improve the workplace experience for employees. Employers are not seeking to create an environment where every employee action is tracked, and

where worker privacy is not valued. Rather, our members are committed to reasonable and ethical use of AI that can assist companies with ensuring a safe workplace, mitigate risks to workers and the business, and assist in compliance efforts with various local, state, federal laws, and regulations, and promote legitimate employer production and quality goals. Additionally, AI tools can be used to help companies boost workforce diversity and build a more inclusive workplace.

**Background**

The capabilities of AI and the pace at which AI is being developed present considerable opportunities and challenges for employers and workers. If properly incorporated into the workplace, AI has the potential to improve the employee experience for all employees and expand opportunities for job candidates who may not otherwise be on the radar of hiring managers. For example, AI can be used to analyze the demographic composition of a workforce and compare that data across industries and regional statistics. These insights allow companies to detect any disparities across race, ethnicity, age, gender, disability, veteran status, and many other factors. Other AI tools may help companies identify additional qualified applicants for employment, better track employee attrition rates, and enhance employee feedback mechanisms which can improve retention, professional development and hiring processes.

In the context of human resources, AI is most effective when it is used to augment, not replace, the core responsibilities of recruiters and hiring managers and the processes that they go through to source job candidates, analyze candidate profiles, and ultimately make hiring decisions. Companies are already incentivized to hire good candidates and to use AI tools appropriately to inform those decisions. A recent assessment by Accenture found that a poor hire can cost companies up to 5x the annual salary of that hire.² AI tools can help expand the talent pool for employers, making it more likely that companies can hire individuals that will be successful and contribute positively to the organization.

However, the complex nature of AI technology and the potential for its misuse also raise a number of risks for companies. For example, a failure to guard against harmful biases in talent identification algorithms, or biases in the datasets that train AI, could undermine efforts to create a skilled and diverse workforce. HR professionals are acutely aware of these risks, given their longstanding responsibilities to prioritize employee safety and privacy and to ensure that any employment decisions are in compliance with labor and employment laws.

To build trust and support worker recruitment and retention, employers are committed to preventing bias in the workplace. Companies are fully aware that any instances of harmful bias in the hiring process can undermine worker confidence and damage the reputation of the business. Reputational damage alone may negatively impact a company’s efforts to assemble and retain a competitive workforce and, according to past studies, may cost companies as much as 10% in additional costs per hire.³ The use of AI, or any other technology, does not inherently diminish or change the commitment of employers to eliminate bias and use AI tools appropriately within their organization. Indeed, use of automated tools can help to reduce bias in recruitment and hiring.

As AI tools further permeate business and society, employers will proactively take steps to ensure that AI algorithms are acting as intended and not creating harmful outcomes. Companies know that their reputation and public trust could be irrevocably damaged if AI tools were

---

² Chambliss, Corey; Vaughan, Kristen. “Next generation talent assessment.” Accenture.

deployed in a manner that caused harm to employees or discriminated against workers and job candidates. Such a loss of trust would set back a company’s ability to use AI, which could make the company less competitive and dynamic in the future.

**Reasonable Use of Automated Workplace Monitoring Tools**

HR Policy Association recently surveyed our members to assist policymakers in understanding how automation is used in the workforce management and surveillance context.

According to the Association’s member survey, conducted in June, most respondents use AI and automated tools in the workplace that are tailored to their respective company’s needs. The tools are mainly used for HR purposes such as to source and screen job candidates and enable employee self-services such as looking up company policies or benefits.

While the majority of respondents indicate that they plan to increase usage of AI and automation in the next year, they do not anticipate freezing hiring for AI-impacted roles. Of significance, companies that utilize AI and automated tools do not use automated tools to make decisions without human input.

Of relevance to the OSTP's request for comment, most respondents indicate that they do not use data from monitoring tools to inform employment decisions. The information is used to provide constructive feedback to employees regarding general performance. Furthermore, most companies provide notice to employees who are being monitored using automated tools, contrary to what this request for comment purports. Finally, a majority of respondents indicated that they only review monitoring data for performance assessment purposes, and that they do not otherwise monitor available information on a continuous or ongoing basis.

Automation can assist employers in achieving several key priorities, including:

**Ensuring Safe Workplaces**

Creating a safe environment for employees and customers is a necessity for any company. Automated monitoring tools can assist businesses with this fundamental responsibility in a much more efficient and effective manner than manual approaches. Indeed, most of our survey respondents indicate that they use automated monitoring tools to track employee movement and location (e.g., staff badges, facial recognition, vehicle monitoring) for safety purposes. For example, a security camera system that utilizes AI technology can be deployed to ensure that no unauthorized personnel enter certain premises, and that the company is able to respond in real time to suspicious behavior. In transportation related or adjacent industries, monitoring tools are essential for tracking employer-owned vehicles operated by employees, both for employee safety and performance purposes. The Request itself cites several ways in which AI may be appropriately used to enhance worker, customer, and community safety. For example, monitoring the speed and acceleration habits of delivery or rideshare drivers can help encourage safer driving habits and lead to fewer accidents or traffic violations. In general, it is essential that employers are aware of whether an employee is endangering themselves or others while on the job. Such information can also be used to rebut improper claims by third parties against companies and their employees in traffic accident matters and provide necessary safety/quality feedback.

---

4 Quote the relevant text.
Identifying patterns of potential misbehavior, including harassment or other abusive behavior, can also be enhanced by automated systems. In certain industries, AI can also be used to monitor and maintain oversight of controlled substances that the organization may manufacture or distribute, thereby lowering the chances that powerful drugs may end up in the wrong hands. For example, automated monitoring tools are essential in healthcare settings, where employees are often charged with handling significant amounts of controlled substances. Losing track of such substances can create significant safety issues for the employer, their employees, their consumers, and the general public. Even something as simple as tracking and ensuring patients are receiving the right drugs and the right doses of such drugs can be better accomplished with the help of automated monitoring tools.

**Ensuring and Measuring Productivity**

Tracking and measuring productivity is not a new concept for employers, and companies have been using technology to assess productivity long before AI became a focus of policymakers. Employers understand, however, that measuring worker performance must be done within reason and not improperly surveil the daily activities of individuals.

As workplaces have increasingly become more digital and employers are adopting hybrid or fully remote long-term work plans, it is essential that employers be able to use automated systems to measure worker performance. New regulations that prohibit or severely disincentivize the use of such tools could prevent employers from tracking progress in a supply chain or from various workstreams that involve multiple departments within an organization.

As noted above, our survey indicates that our member companies do not – at least for productivity and performance measuring purposes – use such tools to constantly and continuously monitor or surveil employees. Instead, data is primarily only reviewed for periodic performance assessments, and generally used to provide constructive feedback and coaching as necessary. Our survey indicates that our member companies generally do not use data from monitoring tools to inform any employment decisions. When this data is used in that fashion, it is generally only used to supplement human input and decision-making, and not as the sole basis for any employment decision. Finally, and perhaps most importantly, those member companies that do use automated systems for monitoring purposes overwhelmingly provide their employees with advance notice of such monitoring.

**Risk Mitigation and Ensuring Compliance with Legal Requirements**

Employers are subject to a host of federal and state laws regarding safety requirements, labor practices, anti-discrimination statutes, and other standards that require companies to have robust compliance systems. Companies must regularly monitor legal and regulatory developments that impact their organization and industry in order to consistently maintain compliance with these laws and regulations.

Employers – particularly larger companies – must regularly collect and analyze vast amounts of data for either recordkeeping or purposes of reporting to a government agency. Automated tools can make these processes more efficient, reduce human error, and improve compliance for companies in every industry. As one law review article from 2010 stated: “Given the scale and complexity of contemporary business institutions and the massive amount of information involved in corporate operations, the types of risk controls that regulation demands simply
cannot function without the data collection, analyzing, and monitoring capacities of integrated computer technology." The automated tools that exist today will only help make risk monitoring and compliance more efficient and effective for employers.

**HR Policy Association Principles**

In 2020, HR Policy Association recommended to our members a set of principles on the use of employee data and AI as a framework and starting point for companies to leverage in their own work environments. Companies understand the need to be open and responsive to their employees and customers regarding AI and any automated tools which a business may use. Given heightened public anxiety over the use and growth of AI, businesses recognize the opportunity they have to lead and ensure that AI can be a force for good in the economy and which can help create a better future for employers and workers.

We encourage OSTP to consider these principles as they develop any final policy recommendations:

- **Privacy and Security**: Most companies maintain privacy policies applicable to current and prospective employees and tailor such policies to comply with jurisdiction-specific privacy regulations in the U.S. and abroad (e.g., the European Union’s General Data Protection Regulation). Principles for the use of data and AI should include a statement specific to employee privacy and security and may explicitly state that data may not be used for the purpose incompatible with the specific purpose for which it was collected without employee consent.

- **Transparency**: The intended uses of data should be able to be clearly understood, explained, and shared, including the impact on decision-making and the processes for raising and resolving any issues. In some cases, this may include an explanation of the algorithms involved in machine learning assisted analysis and how those algorithms are developed and “trained” to analyze employee data.

- **Integrity**: The principle of integrity is interpreted in a variety of different ways by companies according to their culture but is rooted in the concept of “positive intent.” In addition to committing to the use of data in a highly responsible way, companies may also specify that the purpose of all automation and AI is to augment and elevate humans rather than replace or diminish them, and that data usage should be sensitive to cultural norms and customs and aligned with company values.

- **Bias**: Although AI has been touted as the solution to unintended bias in many people-related processes, such as hiring, performance management and promotion, there is inherent risk of unintentional bias occurring within AI algorithms or the datasets used to train them. Principles around data and ethics should commit to continuous monitoring and correction for unintended bias in machine learning.

---

- **Accountability:** Companies should be accountable for the proper functioning of automation and AI systems and for unintended foreseeable consequences arising out of its use. Companies should ensure that everyone involved in the lifecycle of the technology is trained in ethics and that ethics is part of the product development and operation of an automated system. This may include the coders and developers responsible for creating the software, the data scientists responsible for training it, or the management of the company. Further, companies should develop governance and training mechanisms to ensure that automated systems and AI are developed responsibly.

**Substantial Existing Law Already Applies to the Use of AI in the Workplace**

The use of technology in the employment context is already subject to extensive regulation which should be taken into consideration when developing any additional protections. In the United States alone, federal and state laws dealing with anti-discrimination, labor policy, data privacy, and AI-specific issues affect the use of AI in the employment context.

These areas of law include:

- **Anti-Discrimination:** Title VII of the Civil Rights Act prohibits discrimination in the employment context on the basis of race, color, religion, national origin, or sex. An employer can violate Title VII for disparate treatment or disparate impact. Disparate treatment occurs when similarly situated people are treated differently based on a protected class. Disparate impact occurs when facially neutral policies or practices have a disproportionately adverse impact on protected classes. Discriminatory intent is relevant to establish a claim of disparate treatment, but intent is not necessary for claims of disparate impact. Employers are also prohibited from unlawfully discriminating in the employment context based on age or disability due to the Age Discrimination in Employment Act and the Americans with Disabilities Act.

  Liability for discrimination may arise under anti-discrimination laws when employers use artificial intelligence systems that are trained on biased datasets or that infer or otherwise uncover protected class information and adversely impact members of the protected class. With respect to anti-discrimination measures, any new government guidelines should be co-extensive with existing anti-discrimination laws instead of imposing novel obligations that exceed existing law.

  In fact, the U.S. Equal Employment Opportunity Commission (EEOC) recently released a technical assistance document explaining the application of Title VII of the Civil Rights of 1964 in preventing employer discrimination when using automated systems. As that document explains, the 1978 EEOC Uniform Guidelines on Employee Selection Procedures “would apply to algorithmic decision-making tools when they are used to make or inform decisions about whether to hire, promote, terminate, or take similar actions toward applicants or current employees.”

---

In other words, existing law can in many instances be applied to the use of AI in the workplace. Any new guidelines or policy proposals from OSTP or other government bodies should be fully aligned with guidance from the EEOC and other agencies that promulgate AI workplace-related proposals.

- **Labor Laws:** The National Labor Relations Act (NLRA), enforced by the National Labor Relations Board (NLRB), is the cornerstone of American federal labor law and guarantees the right of private sector employees “to organize, engage with one another to seek better working conditions, choose whether or not to have a collective bargaining representative negotiate on their behalf with their employer, or refrain from doing so.” The National Labor Relations Act prohibits employers from interfering with, restraining, or coercing employees’ exercise of Section 7 rights, including spying (i.e., doing something out of the ordinary to observe the activity) or giving the appearance of spying on employees’ union activities.

On October 31, 2022, NLRB General Counsel Jennifer Abruzzo issued a memorandum addressing Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights. In the memorandum, the General Counsel announced she will urge the NLRB to adopt a new framework to protect employees from intrusive or abusive electronic monitoring and automated management practices that would tend to interfere with an employee’s protected activity by vigorously enforcing current law and applying settled labor law principles in a new framework. The General Counsel has also made clear that the NLRB is committed to an interagency approach to these electronic monitoring and automated management practices issues. To that end, the General Counsel signed agreements with the Federal Trade Commission, the Department of Justice, and the Department of Labor which will facilitate information sharing and coordinated enforcement on these issues.

The NLRB has taken the General Counsel’s instruction seriously. On April 11, 2023, the NLRB found that an employer violated the NLRA by creating an unlawful impression of spying when it viewed camera footage of an employee who was on his lunch break, even though the employee was not engaged in protected concerted activity.

While it is important to recognize and monitor these developments, care should be taken by regulators to balance the rights of employers to monitor their workplace for legitimate non-discriminatory reasons with the rights of employees under Section 7 of the NLRA. Specifically, employers should not have to establish any “special circumstances” to implement carefully tailored necessary workplace monitoring policies.

- **Data Privacy Laws:** Data privacy laws at the federal and state level directly affect the use of technology in the employment context. Federally, the Fair Credit Reporting Act (FCRA) regulates, among other things, how consumer reporting agencies use and share consumer information. A “consumer report” is defined as information bearing on a consumer’s credit worthiness, including information related to a consumer’s credit standing, credit capacity,

---

7 https://www.nlrb.gov/about-nlrb/who-we-are
8 https://www.nlrb.gov/about-nlrb/rights-we-protect/the-law/interfering-with-employee-rights-section-7-8a1
10 Stern Produce Company, Inc., 372 NLRB No. 74 (2023)
character, general reputation, personal characteristics, or mode of living. The FCRA requires consumer reports to be used for only permissible purposes, such as for employment. Employers must provide disclosures and obtain consents if using consumer reports.

In addition to the FCRA, employers must also navigate biometric information privacy laws in numerous states. For example, the Illinois Biometric Information Privacy Act (BIPA) prohibits organizations, including employers, from collecting and using biometric information unless they have provided notice and obtained written consent.

Policymakers must be careful to consider these existing laws that can be applied to the use of AI and automated tools, just as they apply to other technologies employers may use in connection with their workforce. Regulators should not rush forward with sweeping, overly prescriptive, one-size-fits-all new rules that will impede investment and innovation in AI, and disincentivize employers from leading efforts to promote responsible uses of automated tools.

**Conclusion**

While automation and AI has generated a number of important and difficult questions regarding its role in the workplace, policymakers should avoid rushing new regulations into place that could stifle investment in such tools and limit the ways the technology can be used to improve the work experience and livelihood of millions of workers. While employers recognize the opportunity that creates for them to operate better workplaces, they also recognize the responsibility that comes with automation deployment and the importance of employee safety and privacy. Employers will continue to lead the way when it comes to developing appropriate automation standards and ethical practices.

Finally, from a public policy perspective, any new regulations considered by federal agencies must be subject to a robust formal notice-and-comment procedure under the Administrative Procedure Act and take the views of all stakeholders into account. Rules based upon unproven theories or insufficient evidence and data would be counterproductive and undermine many of the private sector initiatives currently underway to promote the responsible use of automation. Careful balancing should occur to ensure that employer rights are considered on an equal basis with employee rights.

HR Policy Association appreciates this opportunity to comment and looks forward to serving as a resource on these critical issues. If you have any questions about the Association’s comments, please feel free to contact me at Cbirbal@hrpolicy.org.

Sincerely,

Chatrane Birbal

Chatrane Birbal
*Vice President, Policy and Government Relations*
HR Policy Association
cbirbal@hrpolicy.org
The organization I represent serves people with developmental disabilities. We assist people in locating employment and then continue to support them with the coaching and other assistance they need while employed. We also hire direct support workers to assist people with developmental disabilities who we serve. The comments we are submitting are based on discussions with both groups of workers. People with developmental disabilities have very low rates of employment; some of their comments are based on their concerns of potential issues.

There are two groups of workers who are negatively impacted from worker surveillance as discussed below:

People with developmental disabilities will have problems where their facial expressions are not typical (e.g., people with autism, people with cerebral palsy when speaking) and when they have other physical issues that cannot be measured correctly by worker surveillance systems, particularly Artificial Intelligence (AI) that is generated from more typical workers. In addition, it is likely that in response to worker surveillance, other workers will be less likely to spend any time helping the person with a disability. It is important that any regulations state that for an accommodation related to worker surveillance to be legal, it must be exact in terms of its description and clearly stated what accommodation the person with a disability is granted by the company to receive. It also is important that the hiring process not discriminate against people with disabilities related to facial expressions, ways of expressing themselves, and other characteristics that may be screened for by AI systems.

For direct support staff working with people who have disabilities, it is important to note that the federal government has significant control over this since much of this work is funded through CMS in partnership with state governments. Because of the Affordable Care Act, there is already worker surveillance through the EVV system with clocking in and out. In addition, state governments are likely to increase direct surveillance in response to monitoring surveys and reports they receive from CMS. It is
important to note that the direct support staff crisis will become exponentially worse as there is increasing worker surveillance. Our organization has already found that direct support staff, many of whom have worked successfully for years with people with disabilities, refuse to work for people whose families want a camera present to observe everything. As a result, these individuals with disabilities often go for long periods without staff.

Impacting both groups of workers is the concern about the privacy rights of others where video or audio surveillance is occurring. If direct support workers are under surveillance in the person with a disability’s home, there are significant privacy issues. As employers can electronically store surveillance information, employers become incredibly powerful in having this level of information about their employees. Editing of tapes can lead to misunderstanding or misrepresentation of the meaning of what is happening. For example, we had an employee show us a video of a person with a disability he served that was carefully edited to only show negative behaviors, which turned out to not occur very often. But the tape implied that these behaviors were continuous.

Thank you for this chance to share this information about the impacts of worker surveillance.
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0176
Comment on FR Doc # 2023 12995

Submitter Information

Email: 
Organization: AFL CIO Technology Institute

General Comment

Comment attached

Attachments

AFL-CIO Technology Institute Comment on OSTP Automated Worker Surveillance and Management RFI
Mr. Alan Mislove
Assistant Director for Data and Democracy
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20504

June 29, 2023

Re: Request for Information: Automated Worker Surveillance and Management filed electronically at www.regulations.gov and by electronic mail to workersurveillance@ostp.eop.gov.

Dear Mr. Mislove:

The AFL-CIO Technology Institute (Tech Institute) commends the Executive Office of the President’s Office of Science and Technology Policy (OSTP) for soliciting information on the prevalence and impact of automated worker surveillance and management.¹ Employers have been deploying increasingly sophisticated technologies to monitor workers on and off the job and to hire, control, evaluate, discipline, and even fire workers. These powerful algorithmic monitoring and management tools have frequently been imposed on workers without their knowledge, input, or consent and have significant negative impacts on workers’ privacy, economic security, dignity and autonomy, workplace safety, physical and mental well-being, and the right to form and join unions.

These issues affect tens of millions of workers including the millions of workers represented by unions. The Tech Institute is independent of but affiliated with the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO). The AFL-CIO is a voluntary, democratic federation of 60 affiliated unions representing more than 12.5 million workers across the country in all sectors of our economy. The AFL-CIO is committed to fairness in the workplace and health security for working people and their families. Its core mission is to ensure that working people are

treated fairly and with respect, that hard work is rewarded with family-supporting wages and benefits, and that workplaces are safe.

Employer surveillance and monitoring-driven supervision is not new — time clocks, piece rates, supervisors walking shop floors has long been part of the world of work. Many of these technologies have benign or beneficial purposes such as safety and training, identifying insider cyber threats, and enforcing compliance with corporate policies, but the reality is that the majority of workplace surveillance systems are deployed to control workers and increase productivity. But the increased power and declining costs of advanced digital surveillance powered by mountains of data and computer analytics have fundamentally changed the intrusiveness and control of workers. These surveillance and automated management systems have been deployed for years to control lower-wage workers and have disproportionately impacted women, people of color, and immigrants. The pandemic brought greater visibility to ubiquitous employer surveillance when more tools and techniques were imposed on white collar and remote workers. The accelerated emergence of advanced artificial intelligence capabilities only adds to the urgency of the moment.

The OSTP should launch an all-of-government approach to confront the multiplicity of issues facing workers from automated surveillance and management. Currently, there are few statutory protections for workers from the rapidly emerging risks of digital surveillance and algorithmic management. The existing worker, consumer, and civil rights protections have not kept pace with the deployment of increasingly complex software and technology in the workplace and the patchwork of privacy protections largely predate the internet era. The Executive Director of Workplace Fairness told the New York Times that “The law gives employers a level of freedom — a pretty high level of freedom — to do surveillance, not just in the workplace but outside of the workplace.” Agencies are just beginning to address how to enforce existing labor and employment law in the digital environment of automated surveillance and management. The U.S. Department of Labor has just begun to evaluate the impact of algorithmic hiring software and will begin assessing algorithmic management and workplace safety in warehouses in 2024.

Surveillance and algorithmic management are distinct but interrelated employer strategies designed at their most basic level to control workers. The current surveillance technologies allow for continuous, real-time, location, activity, biometric and even emotive monitoring at work and even off the clock. By itself, this intrusive level of surveillance dehumanizes workers, infringes on their privacy, heightens job dissatisfaction, causes high levels of stress, and can interfere with, restrain or coerce employees in the exercise of their right to engage in union activity and/or other protected concerted activity.

Automated or algorithmic management uses the data employers collect from worker surveillance as part of the inputs for supervisory software that recruits and hires workers, assigns tasks and schedules, evaluates and rates the performance of workers, and imposes discipline (or more rarely

---


rewards) and even terminates workers. The deployment of these systems has been associated with higher workplace injuries from productivity-prodding work intensification, deskilling of workers whose job autonomy is diminished, increased economic precarity from algorithmic pay and schedule changes, and racial and gender bias and discrimination in hiring and promotion. Millions of workers are affected by the negative impacts of these technologies. The examples in this comment are illustrative, not a comprehensive assessment of the impacts on workers, workplaces, and work.

The Tech Institute urges the OSTP to craft a robust, government-wide agenda to protect workers from the harms of automated surveillance and management. These tools could and should be used to make jobs safer, less physically punishing or monotonous, and build new skills and new careers for workers — especially if workers have a meaningful seat at the table for the development and deployment of these technologies.

Labor unions have been at the forefront of building more worker-centered approaches to the adoption of new technologies that improve workplace conditions. But it is critical that the OSTP lead an effort to shield workers from the known and emerging risks of these technologies. The near total lack of guardrails or oversight has allowed employers to deploy automated surveillance and algorithmic management with little regard for the impacts on workers. These technologies have contributed to making workplaces more dangerous, more stressful, more dehumanizing, lower-paid, privacy eroding, and harder for workers to exercise their rights to form and join unions.

This comment describes the rise, prevalence, and impact of automated surveillance and algorithmic management on work, workers, and the workplace and the need for OSTP to build a government-wide strategy to address these harms to workers:

I. **Introduction:** Documents the history of worker surveillance and the rise of digital surveillance and algorithmic management; how the adoption of these new advanced technologies leads to job losses, deskilling, and the fissuring of employment relationships; and the disparate impact these technologies are having on women and people of color.

II. **Workers face ubiquitous surveillance by their employers on and off the job:** Details the new technological advances and their ubiquity and basic risks to workers; the prevalence in the workplace and worker distrust of workplace surveillance; and describes the technologies and techniques used by employers to monitor workers on and off the clock.

III. **Workers are harmed by constant automated surveillance:** Describes how surveillance alone can interfere with, restrain or coerce employees in the exercise of their right to engage in union activity and/or other protected concerted activity; create high-stress workplaces that contribute to health harms, undermine trust, and reduce job satisfaction; and infringe on workers privacy by monitoring during off-work hours, inappropriately using biometric information, and collecting and commodifying personal data on workers.
IV. Automated (or algorithmic) management increasingly controls and harms workers: Describes automated, algorithmic management systems and the broad impacts on workers; the rise of algorithmic management and its prevalence in the workplace; how algorithmic management can harm the physical and mental well-being of workers, contribute to de-skilling, reduce worker autonomy and dignity, and economic insecurity; and the total opacity and unaccountability of these algorithmic systems leaving workers with little recourse to unfair or biased decisions.

V. Case studies on the worker harms of algorithmic management: Describes how the bias in recruiting and hiring algorithms; how task assignment and productivity monitoring increases work intensification that can compromise workplace safety; how task assignment can also lead to de-skilling compromising the quality of services; how algorithmic scheduling exacerbates economic precarity; and how algorithmic discipline threatens the economic security of workers.

VI. Collective bargaining over automated workplace surveillance and management technologies should be widely encouraged: Describes how collective bargaining agreements are the most effective tool to incorporate worker perspectives in technological development and implementation before employers impose these digital technologies that can harm workers.

VII. Conclusion and recommendations: Urges the OSTP to take an all-of-government approach to addressing the known harms of automated worker surveillance and algorithmic management.

I. Introduction

The current wave of digitally enhanced worker surveillance and algorithmic management are a new chapter in an old story for workers. It represents an exponentially more powerful exercise of employer control over workers with more powerful technological tools. The new technologies have leveraged employer power to amplify the long-standing corrosive threats to workers through automation-associated job losses, deskillling of workers that undermines worker dignity, and fissuring the employment relationship by turning workers into contractors. The negative impact of these trends — along with economic precarity and workplaces that harm workers physical health and mental well-being — has disproportionately impacted women, people of color, and new immigrants that both face algorithmic bias and are concentrated in the lower-wage jobs where these technologies are more commonly deployed.

Employers have long measured workers’ performance and surveilled them in the workplace. Supervisors walk shop floors and detailed production metrics are tracked. The rise of such “scientific” management has its origins in the Industrial Revolution, which introduced meticulous monitoring of specific worker tasks, collection of productivity data, and close monitoring of workers. These new workplaces included punch clocks, production quotas, and shift-based work periods. The combination of worker surveillance and worker productivity metrics became a

*Hickok & Maslej 2023 at 3.*
mainstream tenet of Frederick Taylor’s scientific management in the late 19th century. Taylorism planned out detailed instructions for the tasks and steps workers were to perform (essentially as human machines in an industrial process), performed time studies to set wage rates, and legitimized and justified the rise of a new managerial class.

The U.S. labor movement and the enactment of U.S. labor and employment laws grew out of the dehumanizing treatment of workers by Taylorism. The ideas of Taylorism — close monitoring and measuring of work and workers — have entered a digital era. In the 1970s and 1980s, the adoption of office computer systems and algorithmic controls of robotic manufacturing systems began a digitization of control. The current wave of what some have called “digital Taylorism” is driven by powerful surveillance and data-processing tools that control workers, suppress wages, and make it harder to form unions. Many workers are continuously monitored in real-time, have their tasks assigned by tablet or device, are prodded to increase work more intensively (potentially contributing to workplace injuries), have their performance rated by computer algorithms, and get disciplined or even fired by electronic messages. Employers can oversee more workers without human oversight and impose even more rigid standardization, task decomposition, and performance metrics of work. These forces have accelerated the automation, deskilling, and job fissuring that harms workers and disproportionately harms women, people of color, and new immigrants.

a. Automated worker surveillance and management fuel automation-driven job losses, deskilling and fissuring

Automated worker surveillance and algorithmic management can lead to job losses, de-skilling of occupations, reduced autonomy and job satisfaction, and the erosion of economic stability for working families that contribute to the rising economic and racial inequality.

Automation of surveillance and management contributes to job losses: Labor organizations have been helping workers navigate the adoption of the new technologies and innovations that changed the nature of work. Some technologies have made workplaces safer, reduced physical or repetitive burdens, or created new occupations. But automation and new technologies, when developed and implemented without meaningful worker input, also eliminate jobs, de-skill occupations, reduce autonomy and job satisfaction, and disrupt and erode the economic stability for working families that contribute to rising economic and racial inequality.

Technology-driven worker replacement has been a persistent concern for generations and the current wave of technological change sweeping the workplace — especially through the adoption of

---


artificial intelligence — mirrors some of the prior technological seismic shifts. These transformations can eliminate occupational categories and if workers are not re-skilled or upskilled to jobs with comparable economic opportunity, millions of working families can have their economic security upended.

The millions of manufacturing workers that lost their jobs due to trade deals and office workers that lost their jobs to desktop computers faced dramatically declining earnings and the training programs were insufficient to provide the foundation of needed skills or opportunity for working families. The telephone industry’s transition from manual operators to mechanical switching in the 1920s to 1940s eliminated half the telephone operator jobs, and while younger women shifted to comparably paying clerical, retail, and restaurant jobs, more senior workers either left the workforce or took lower-paying jobs.

The emergence of generative artificial intelligence (AI) has already raised concerns about substantial job losses. The impact is likely to be similar to the computerization of office work. In the early 1980s, the adoption of office computers, word processing software, and advanced photocopying displaced a hundred thousand clerical, secretarial, and stenographic jobs, and by 1990, the share of these workers in the economy declined for the first time in the twentieth century.

The warnings of AI-driven job losses are mounting and some workers are already losing jobs to a technology that has been available only a few months. Goldman Sachs estimated that AI would eliminate or degrade 300 million jobs globally and the World Economic Forum predicted that 25 percent of all jobs could be affected. A 2023 OpenAI and University of Pennsylvania study estimated that generative AI could eliminate 15 percent of U.S. jobs and another 19 percent of workers could have half of their work tasks impacted by the technology. Some workers have already lost their jobs as copywriters and digital content providers have been replaced by ChatGPT. IBM has recently announced that it will halt hiring for 7,800 existing jobs it believed could be replaced by AI.

The emergence of generative AI that could replace or de-skill writers prompted the Writers Guild of America (WGA) to include three AI demands in its 2023 contract negotiations to regulate the use of artificial intelligence on covered projects — that AI cannot write or rewrite literary material (such as scripts), cannot be used as source material (such as concepts, books, or plays), and covered material cannot be used to train AI — but the studios rejected these demands.

---

14 Kelly, Jack. “Goldman Sachs predicts 300 million jobs will be lost or degraded by artificial intelligence.” Forbes. May 31, 2023; Kulerlein, Sophie. “Nearly 25% of jobs are set to be disrupted in the next five years — and A.I. could play a key role; World Economic Forum,” CNBC. May 2, 2023.
reasonable measures and instead only offered annual technology meetings; the contract talks broke down and the WGA went on strike in May 2023.\footnote{Klee, Miles and Krystie Lee Yandoli. “Why striking Hollywood writers fear an Ai future.” Rolling Stone. May 5, 2023.}

**Algorithmic management deskills and can lead to the replacement of workers:** Automation does not always replace workers, it often changes the tasks and activities workers perform and deskills workers into narrower occupational tasks. The adoption of the new technologies transformed workers into cogs that accommodate the new technology or systems, reducing the skill set required, the wages paid, and worker autonomy, job satisfaction, and dignity.\footnote{Nunes, Ashley. “Automation doesn’t just create or destroy jobs—it transforms them.” Harvard Business Review. November 2, 2021}


Algorithmic management task-assignment that minutely directs worker activity can become easy to automate and slash jobs. For example, the Amazon warehouse workers driven by handheld productivity-prodding devices also work in coordination with advanced robots.\footnote{Del Rey, Jason. “Amazon’s robots are getting closer to replacing human hands.” The Verge. September 27, 2022; Baramuki, Chris. “How algorithms run Amazon’s warehouses.” BBC. August 18, 2015.} The algorithmic management tools drive workers to automaton-like task performance while the company is developing robots to replace these very same workers. In the passenger-transport sector some autonomous technology developers want to convert skilled, licensed drivers into “monitors” while the vehicle drives itself. This deskilling makes it easier for employers to fire workers because each worker has a smaller skill set, making them more easily replaceable.

**Algorithmic management and fissuring of the employment relationships:** Companies have deployed new algorithmic management technology to expand the fissuring of workplace relationships, where employers outsource or subcontract workers without maintaining an employment relationship and the legal protections they afford workers. One-fifth of US workers toil in fissured workplaces where companies have outsourced their workforces to subcontractors or converted their workforce into independent contractors. In both circumstances, workers receive low-pay and paltry benefits, and in the case of workers classified (and often misclassified) as independent contractors, they receive none of the labor law protections that employees receive, and no right to form unions.\footnote{Weil, David. “Understanding the present and future of work in the fissured workplace context.” Russel Sage Foundation Journal of the Social Sciences. Vol. 5, No. 3. December 1, 2019.}

This has been happening for decades. But the platform companies that employ “gig” workers pioneered the AI-based algorithmic management task assignment strategies to scale up the management of a large number of geographically dispersed workers.\footnote{Lippert, Isabell, Kathrin Kirchner, Martin Wiener. (Lippert, Kirchner, & Wiener 2023). “Context matters: The use of algorithmic management mechanisms in platform, hybrid, and traditional work contexts.” Proceedings of the 56th Hawaii International Conference on System Sciences. 2023 at 5282.} This both transformed
algorithmic management adoption and accelerated the fissuring of workers from the protections of employment. These platform companies launched an armada of ride-hail and delivery drivers, home health aides, data processors, and other workers directed by smartphone apps, many of whom are routinely misclassified as “independent contractors” and do not get the protections they justly deserve as employees.\textsuperscript{25}

\textbf{b. Automated worker surveillance and management has disparate impacts on women and people of color}

The significant negative effects of workplace surveillance and algorithmic management are primarily borne by low-wage workers that perform hourly or shift work in restaurants, retail stores, warehouses, hotels, and healthcare facilities where their jobs tasks are easily quantified (and thus measured and evaluated) by digital systems.\textsuperscript{26} And employers disproportionately use digital surveillance and algorithmic management tools on lower-income workers and workers of color.\textsuperscript{27}

Long-standing patterns of occupational segregation mean that women, people of color, and immigrants are more likely to be employed in these lower-wage workplaces where they are continuously monitored and algorithmically controlled.\textsuperscript{28} A 2023 study estimated that Black, women, and younger workers were more likely to face workplace surveillance because of their lower skill and wage levels and lower job autonomy.\textsuperscript{29} Not only are women and people of color more likely to be electronically monitored at work, the use of controlling surveillance can increase social inequality — the monitoring benefits the employer but does not provide any additional protection for workers from discrimination or harassment.\textsuperscript{30} The harms of these digital technologies on disadvantaged workers amplifies the existing economic and racial inequality and power imbalance.\textsuperscript{31}

The increased use of automated tools to screen job applicants, evaluate candidates, and even assess video interviews can replicate societal bias and make it harder for people to secure jobs. Hiring systems can replicate existing preferences that reinforce racial and social biases that perpetuate occupational segregation and inequality.\textsuperscript{32} For example, a 2019 study found that Facebook’s job advertisements for janitors and taxi drivers were overwhelmingly pushed to people of color and

\begin{itemize}
  \item Hickok & Maslej 2023 at 4.
\end{itemize}
advertisements for nurses and secretaries were shown to women. The purportedly facially neutral application of algorithmic human resources decisions can have disproportionate or disparate impact on people of color, women, people with disabilities, older people, and new immigrants.

People know and worry about the risks of automated discriminatory treatment — especially women and people of color. More than half of people (57 percent) are worried that AI will discriminate or demonstrate bias and nearly two-thirds (65 percent) worried that AI tools would harm groups or individuals, according to a 2023 Ipsos poll. Black workers and younger workers were far more likely to think that their work and non-work hours were tracked by their employer (45 percent of Blacks versus 27 percent of whites; 40 percent of workers 18-29 years old versus 28 percent of those 43-64 years old).

II. Workers face ubiquitous surveillance by their employers on and off the job

Technological advances and falling costs have made nearly constant surveillance the reality for millions of workers. The advent of more powerful and cheap digital surveillance technologies has enabled and emboldened employers to deploy increasingly intrusive surveillance systems. Employers are adopting advanced surveillance to monitor workers on the job continuously and in real-time and even track workers outside the workplace. This intrusive practice has been supercharged by artificial intelligence systems that have made surveillance more prevalent and powerful. This surveillance is often unknown to workers and companies need not receive workers’ consent; the surveillance data is owned by the employer which can share or sell this data without workers’ approval.

At root, worker surveillance is about control. There are a number of seemingly benign or even laudable workplace monitoring rationales (policing internet misuse and identifying insider cyber threats, protecting corporate data and proprietary information, enforcing compliance with corporate policies), but the reality is that the majority of workplace surveillance systems are deployed to control workers and increase productivity. For example, some surveillance tools can be helpful for safety in limited circumstances, especially when workers are working alone (such as hazard sensors and alarms), but far more frequently these “safety” monitoring tools are response or reporting tools, not prevention tools, and these limited safety purposes are used to justify function creep and implement more surveillance rather than fixing the workplace hazard.

---

Yang 2020 at 8 to 11.
Ipsos. “We are worried about irresponsible uses of AI.” April 28, 2023.
Hickok & Maslej 2023 at 4.
Bernhardt, Krege & Suliman 2021 at 18.
Mehl 2023.
Ball 2021 at 28; Hickok & Maslej 2023 at 3.
The data and information employers collect through automated worker surveillance fuels the algorithmic management tools that rely on a constant stream of real-time data on workers to track performance and productivity and control the pace of work and work intensity. Digital surveillance technologies give employers granular, continuous, and real-time data on workers’ activities and has enabled employers to more easily monitor workers when they are off-the-clock during their non-working life. Companies monitor worksites with cameras, handheld or wearable productivity and location trackers, keystroke and mouse logging, biometrics like fingerprints. But it also can include surveillance of workers outside of the workplace, including GPS location tracking of workers off the clock, monitoring social media activity, and assembling detailed dossiers of personal information unrelated to the workplace.

Workplace surveillance is common in every industry and affects all kinds of workers, whether they know it or not. A recent New York Times report found that workplace surveillance was ubiquitous from low-wage workers at warehouses and retail outlets to white collar office workers including lawyers and architects that experience “growing electronic surveillance over every minute of their workday.” This workplace surveillance affects nurses and home health workers, teachers, warehouse workers, fast food workers, retail workers, and more.

And it’s nearly impossible for workers to avoid this employer monitoring, even if they know about it. Surveillance tools are imposed upon workers who generally lack the power to resist their deployment. Workers cannot avoid automated surveillance that is essentially a take-it-or-leave it condition of employment — it is a false choice between their livelihood or their privacy. A security company advised employers that “even if companies give employees a choice about whether or not they want to participate [in waiving privacy rights], it’s not hard to force employees to agree.”

The surveillance itself — even without algorithmic management — has significantly negative effects on workers. The next section describes how constant, intrusive surveillance demoralizes and

---

iv. Hicken & Maslej 2023 at 5.

Mehl 2023.
stresses workers, undermines their privacy, and harms the right to form and join unions. The Washington Center for Equitable Growth concluded that the current wave of digital workplace surveillance “exacerbates exploitative workplace practices, but also undermines worker power and contributes to increasingly worse wages and working conditions.”

a. Prevalence and unpopularity of workplace surveillance

There is broad agreement that electronic workplace monitoring is increasing, but there is no official or comprehensive assessment of the prevalence of digital surveillance in the workplace. Surveys of workers and employers suggest that the share of workplaces and workers that are electronically monitored is increasing and that more types of electronic surveillance are being deployed. In 2019, the Gartner consulting firm reported that more than half of 239 surveyed large employers were using some form of advanced surveillance to monitor their workers — including reading emails and social media posts and tracking computer activities. The expansion of worker surveillance exhibits “function creep,” where marginal increases in surveillance and data collection become normalized so that employers are willing to deploy more intrusive technologies even without the knowledge or consent of their workers.

The pandemic indisputably increased worker surveillance, but, in many respects, it merely brought far more office workers under employers’ electronic eye. Electronic surveillance of lower-wage workers has been commonplace for years. Worker surveillance — and employers’ willingness to deploy increasingly intrusive monitoring techniques — soared during the pandemic. A 2021 survey found that 78 percent of employers were using software to monitor their remote workers.

Workers are distrustful of surveillance. They know that it is really a proxy for managers’ trust in their employees — more and more intrusive monitoring suggests to workers that managers do not trust their commitment, competence, or honesty. Workers have strong emotional concerns about privacy violations, particularly how biometric and location data are collected and used. A 2023 Pew Research poll found that 61 percent of U.S. adults opposed employers tracking workers’ movements on the job, 56 percent opposed tracking desk workers activities, 52 percent opposed tracking how often workers took breaks, and 51 percent opposed tracking exactly what workers are doing on their work computers.

Remote workers worried especially about how their employers could surveil their homes and family. A 2022 survey of people who worked from home during the pandemic found that workers were most concerned about video or images of their homes being included in their employer’s

---

55 Zickuhr 2021 at 6.
57 Stark, Stanhaus & Anthony 2020 at 1076.
58 Ball 2021 at 7.
60 Ball 2021 at 12.
61 Ibid. at 35.
monitoring and they were concerned that the level of monitoring would continue even when they returned to the office.\textsuperscript{63}

\textbf{b. The new techniques and technologies of workplace surveillance}

Employers are deploying an array of new or advanced surveillance technologies to monitor workers on the job and even outside of work hours. Many workplaces use multiple types of surveillance to track workers’ movement and location on the job, track their movements on the road even when not working, their activity and task performance, intimate physical biometric data like pulse rates and sleep patterns, and personal information for predictive forecasting, and more. Some of the more common automated surveillance techniques and strategies include:

\textbf{Location tracking in the workplace:} Employers track the physical location of workers through sensors, cameras, wearable devices like badges and wristbands, and handheld devices like scanners.\textsuperscript{64} Occupancy tracking sensors can count the number and persistence of employees (and customers) in a specific location.\textsuperscript{65} This monitoring can be used to control workers, direct their work activity, and be used to monitor workers for exercising their right to engage in union activity and/or other protected concerted activity.

\textbf{Geolocation tracking off the worksite:} Some companies require workers to download apps onto their personal mobile phones that track location and other information, even outside of working hours.\textsuperscript{66} Drivers for delivery and trucking companies are remotely monitored for real-time geolocation and other telemetric information like speed, braking, and fuel use.\textsuperscript{67} Location monitoring is common for workers in utility, cleaning, homecare, mental health, security, mass transit, trucking, warehouses and road construction.\textsuperscript{68} These tools are intended to keep track of remote, on-the-road, and route-based workers, but they can pose risks to worker privacy when their travels off work hours can be tracked by their employers. The \textit{New York Times} documented how location tracking apps can reveal personal information including trips to medical appointments, romantic partners, or addiction recovery meetings.\textsuperscript{69} Most strikingly, in a post-\textit{Roe} America, location tracking, internet search histories, and other digital footprints can create legal peril for women seeking abortion services in many states.\textsuperscript{70}

\textbf{Video and audio surveillance:} The technological advances in digital video and video analytics make it possible for employers to monitor and analyze real-time video feeds from workplaces.\textsuperscript{71}

\textsuperscript{63} Vitak, Jessica and Michael Zimmer. (Vitak & Zimmer 2021). Marquette University. \textit{“Surveillance during and after the Covid-19 pandemic.”} Computer Science Faculty Research and Publications No. 68. 2021 at 4 to 5.

\textsuperscript{64} De Stefano & Tacs 2022 at 23; Gagné, Marylène et al. (Gagné et al. 2022) \textit{“How algorithmic management influences worker motivation: A self-determination theory perspective.”} Canadian Psychology. April 2022.

\textsuperscript{65} Mehl 2023.

\textsuperscript{66} Hickok & Maslej 2023 at 6.


\textsuperscript{68} Ball 2021 at 26.

\textsuperscript{69} Valentino-DeVries, Jennifer et al. \textit{“Your apps know where you were last night, and they’re not keeping it secret.”} \textit{New York Times}. December 10, 2018.

\textsuperscript{70} Brandon, Russell et al. \textit{“The biggest privacy risks in post-Roe America.”} \textit{The Verge}. June 27, 2022.

\textsuperscript{71} Berghaardt, Kresge & Suleiman 2023 at 6; Gagné et al. 2022.
Some employers embed microphones into workplace badges that capture workers’ conversations.\textsuperscript{72} Being under constant video surveillance can be stressful and demeaning. Nannies report undisclosed nanny-cams even in the private living quarters of live-in domestic workers.\textsuperscript{73} Women and people of color distrust employer-imposed camera surveillance, especially if it utilizes facial recognition that can disproportionately target (and misidentify) women and people of color (see biometrics below).\textsuperscript{74}

**Performance monitoring devices:** Automated surveillance is commonly used to collect data for algorithmic productivity monitoring and evaluation. Handheld devices provide continuous, real-time data to employers about worker productivity, work-speed, and time-on-task and allow managers to prod them to work harder and faster.\textsuperscript{75} Some wearable surveillance wristbands vibrate to press workers to perform more optimally when they do not meet targets or are time-off-task for too long.\textsuperscript{76} A 2023 European Commission survey found that mobile devices, including phones and tablets, were increasingly used to surveil and control physical work, and that production workers had the highest level of invasive scrutiny.\textsuperscript{77}

**Surveillance of office workers:** Employers of office workers from administrative assistants to attorneys monitor worker performance and activity through their computers and devices. This surveillance — whether in an office setting or remotely — functions the same way as having a supervisor walk shop floors or offices to make sure that workers are busy.\textsuperscript{78} Employers can monitor keystrokes, mouse tracking, application use, internet web history, idle time, and web cameras and microphones.\textsuperscript{79} Some employers required remote workers to download performance assessment software and to give them access to their computer cameras and microphones while they were working from home.\textsuperscript{80} This allowed some employers to access live video or snapshots of workers’ homes by accessing their web cameras.\textsuperscript{81}

**Biometric monitoring from facial recognition to fingerprints:** Employers are increasingly using biometrics (software that identifies individuals through unique physical characteristics) to monitor workers and improve security. Biometric monitoring can include facial recognition, fingerprint scans, voice recognition, eye-scanners, palm prints and hand geometry, and gait identification.\textsuperscript{82} While technologies like fingerprint scanners are primarily used for security (such as secure computer logins, biometric door locks, or transaction confirmation), facial recognition technology has been integrated with video surveillance and other sensors.\textsuperscript{83} The racial and gender biases and errors in facial recognition are well-known and are encoded into the software and the overwhelmingly white and male photo datasets that train the systems.\textsuperscript{84} More than one-third of facial recognition matches were incorrect for women of color — nearly half the matches for women

\textsuperscript{72} Bernhardt, Krege & Suliman 2021 at 6.
\textsuperscript{73} National Domestic Workers Alliance communication with AFL-CIO Technology Institute. June 2023.
\textsuperscript{74} Ball 2021 at 27.
\textsuperscript{75} Nguyen 2021 at 16; De Stefano & Taes 2023 at 23.
\textsuperscript{76} Jarrahi et al. 2021 at 5.
\textsuperscript{77} Fernández-Macias et al. 2023 at 25 to 26.
\textsuperscript{78} Vitak & Zimmer 2023 at 32.
\textsuperscript{79} Gagne et al. 2022; De Stefano & Taes 2023 at 24; Jarrahi et al. 2021 at 5
\textsuperscript{80} Nguyen 2021 at 3.
\textsuperscript{81} Ball 2021 at 12.
\textsuperscript{82} De Stefano & Taes 2023 at 23 and 24; Mehl 2023.
\textsuperscript{83} Mehl 2023.
\textsuperscript{84} Stark, Stanhaus & Anthony 2020 at 1075.
with the darkest skin have been erroneous — compared to an error rate of below 1 percent for white men.\footnote{Hardesty, Larry. Massachusetts Institute of Technology. “Study finds gender and skin-type bias in commercial artificial intelligence systems.” February 11, 2018.} The built-in bias, error rates, and civil and human rights implications caused both Amazon and IBM to suspend their facial recognition software programs.\footnote{Ivanova, Irina. “Why face-recognition technology has a bias problem.” CBS News. June 12, 2020.}

**Collecting data dossiers on workers:** Some employers collect personal, financial, consumer, or social media data on their workers and aggregate it into the automated surveillance systems for security purposes, to develop predictive models on worker retention or performance, or to identify workers who are sympathetic to unions or critical of the employer. Employers can purchase data on their employees from data brokers that can provide credit reports, social media activity, and other pieces of individualized consumer data that are widely available.\footnote{Bernhardt, Kresge & Suliman 2021 at 6.} The combination of workplace surveillance and data mining allows employers to examine workers’ thoughts and feelings (reading emails and social media posts), track their location, follow the activities and tasks they perform, examine individualized biometric data, and generate rich troves of permanent data supervisors can exploit and employers can commodify that goes far beyond mere performance assessments.\footnote{Ball 2021 at 17.}

Employers also can deploy software bots that track companies or individuals on social media platforms, including postings, mentions, clicks, hashtags, and likes.\footnote{Mehl 2023.} Some companies are monitoring social media posts to evaluate workers’ mental health.\footnote{Vitak & Zimmer 2021 at 4.} The security company Kisi has named social media monitoring software among “the most controversial group of tools.”\footnote{Mehl 2023.} The profiling and personal data collection on workers can significantly infringe on their privacy but also can be used to identify union organizers and union supporters and be used to interfere with, restrain or coerce workers right to form and join unions.

**Wellness and emotive monitoring:** Employers are deploying some of these technologies to assess the emotional state and mental and physical health of their workers. Some employers are collecting continuous data from wearable monitors on blood type, heart rate, blood pressure that can determine worker mental or physical stress levels.\footnote{De Stefano & Tacs 2023 at 24 to 25.} Some employers encourage “wellness” or fitness apps and wearables, such as step counters or sleep tracking, which can raise significant privacy and health bias concerns.\footnote{De Stefano & Tacs 2023 at 23 and 24.} Some employers are using software to analyze video and audio data to make emotive assessments of job candidates or evaluate the mental or emotional health of their workers.\footnote{Ball 2021 at 25; Nguyen 2021 at 3 and 19.} These emotional scoring systems merely replicate the flawed and discriminatory elements of the facial recognition software that these systems are built upon.\footnote{De Stefano & Tacs 2023 at 24 to 25.} A 2023 Pew poll found that 70 percent of people opposed using facial recognition software to assess people’s expressions — nearly three-quarters of people (73 percent) worried about misinterpreting expressions and more than half (53 percent) worried workers would be misidentified.\footnote{Zickuhr 2021 at 16.}
Importantly, these “wellness,” biometric tracking and wearable tools are often used by employers to blame the worker as an individualized approach to personal health and movement monitoring, rather than fulfilling their preventive obligation under the law to provide a safe workplace and maintain a workplace free from harm (See Occupational Safety and Health Act). For example, workers may be required to undergo biomonitoring/tracking at the same time that the employer has failed to repair a gaping hole in the floor or control exposure to toxic dust. In other cases, shift workers have been blamed for not getting enough sleep before work, even though their shift schedules disrupt their sleep cycles (poor work organization). These surveillance tools have not been shown to be effective to reduce work-related injury, illnesses, and fatalities. They instead are used to discipline workers and have not been used in ways that actually prevent hazardous exposures and improve working conditions. At the same time, where technology could have been developed and deployed to improve these outcomes and save lives (such as data collection and tracking to identify trends on work-related injuries and illnesses, more advanced engineering controls to prevent exposure to carcinogens at work, and work re-organization tools instead of increasing work pace), it has not been developed or employers have refused to implement these technological measures.

### III. Workers are harmed by constant automated surveillance

Constant surveillance erodes worker privacy, dehumanizes workers, contributes to declining job satisfaction, amplifies a widening power asymmetry between workers and employers, and is used to violate the right to form and join unions. ⁹⁷ Many of these harms are unquantifiable, like the loss of privacy and demoralization, but impose real costs on workers. For example, surveillance has been associated with higher stress levels and associated health harms for workers. And the data derived from surveillance is not only captured by employers, it is commodified and sold in the same way that consumer data is marketed. Workers often do not know of or consent to this data collection and do not own or control the personal information that is collected and potentially sold by their employers.

The academic literature has documented that digital and automated surveillance has been associated with negative impacts including worker health and psychological stress, declining motivation and job satisfaction, increased turnover, reduced privacy and trust, lower worker autonomy, increased data security risks, and legal exposure from unethical monitoring. ⁹⁸ Noted law firm Skadden, Arps has advised employers that surveillance and algorithmic management posed legal risks including “invasion of privacy, unfair labor practice charges, discrimination, unpaid wages and overtime and workplace injuries.” ⁹⁹

Surveillance alone — not including the interrelated negative impacts of algorithmic management — can pose real harms to workers. The advanced digital surveillance tools make it far easier for employers to identify workers that support unions and workers’ rights, which can prevent workers from exercising their rights to form unions. The constant workplace surveillance is stressful,

⁹⁸ Sultana & Alam 2022 at 271; Ball 2021 at 7.
Automated Worker Surveillance & Management OSTP RFI

contributes to health harms for workers, undermines worker trust and job satisfaction. This surveillance also infringes on workers’ privacy by tracking workers during non-work hours, improperly using biometric data that can be racially biased, and assembling and commodifying personal information on workers.

a. Employer surveillance threatens workers’ rights to form unions

Employers use advanced surveillance technologies to monitor workers and their social media presence to find union organizers and labor activists, identify workers that support unions and labor rights, and to spy on workers unionization efforts. This surveillance can be used to interfere with, restrain, or coerce employees in the exercise of their right to engage in union activity and/or other protected concerted activity protected under the National Labor Relations Act (NLRA). Surveillance can significantly impair or negate employees’ ability to engage in protected activity and keep that activity confidential from their employer, if they so desire.

Employers’ use of workplace and, especially, off-work surveillance combined with the big data collections of personal information gives a “sophisticated picture of what workers are doing and how they feel about their work,” according to a *Saint Louis University Law Journal* article. Although spying on organizing efforts and anti-union coercive pressure violates Section 8(a)(1) of the NLRA, artificial intelligence-driven worker surveillance has been used to identify potential union support and organizing activity and intimidate workers. The mere presence of intrusive surveillance can deter worker-to-worker conversations, as trust and time are eroded by oppressive monitoring — conversations about their lives, about their workplace, and about forming unions.

**Direct surveillance of workers and worker activity used to violate the right to form unions**: Employers use surveillance software tools to determine workers’ union sympathies and potentially exert illegal pressure to discourage workers from forming or joining unions. A 2022 memo from the National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo recognized as troubling “the potential for omnipresent surveillance and other algorithmic-management tools to interfere with the exercise of Section 7 rights [to form or join unions] by significantly impairing or negating employees’ ability to engage in protected activity and keep that activity confidential from their employer.”

There are many examples of this kind of direct anti-union worker surveillance. Walmart patented an audio surveillance system that could monitor customer interactions but could also spy on and suppress protected worker conversations about the company and worker organizing activities.

Amazon’s Whole Foods has used heat maps and predictive algorithms to track locations that were estimated to be high-risk for union activity. McDonalds has operated an intelligence team that

---

101 Constantz 2021.
102 Garden 2018 at 66.
104 Garden 2018 at 65.
105 Constantz 2021; Peters, Jay. “*Whole Foods is reportedly using a heat map to track stores at risk of unionization.*” *The Verge.* April 20, 2020.
monitored Fight for $15 organizers, which McDonalds employees were active in the campaign, and which workers and locations were interested in forming unions.\footnote{Franceshi-Bicchierai, Lorenzo and Lauren Kaori Gurley. "McDonald’s Secretive Intel Team Spies on ‘Fight for $15’ Workers, Internal Documents Show," Vice. February 24, 2021.}

Meta’s Facebook Workplace intranet messenger tool offers employers the ability to monitor and block workers’ posts based on their content, and Meta promoted the tools ability to forbid the word “unionize” (although the company subsequently deleted the presentation and apologized for the anti-union example).\footnote{Fang, Lee. “Facebook pitched new tool allowing employers to suppress words like ‘unionize’ in workplace chat.” The Intercept. June 11, 2020.} Amazon developed plans for an automatic word monitor on internal chat apps that would ban terms relevant to working conditions and concerted action, such as “union,” “grievance,” “pay raise,” “unfair,” and more.\footnote{Klippenstein, Ken. “Leaked: New Amazon Worker Chat App Would Ban Words Like ‘Union,’ ‘Restrooms,’ ‘Pay Raise,’ and ‘Plantation.’” The Intercept. April 4, 2022.}

\textbf{Surveillance of workers’ personal social media presence stifles right to form unions:}

Some employers are snooping on workers’ social media accounts to find unfavorable opinions of the company, determine worker discontent and union sympathies, and identify whistleblowers. A 2012 study found that about 100 people filed NLRB charges of unfair labor practices for being fired or disciplined for social media posts, including for posts the NLRB determined were protected activity under the National Labor Relations Act (although most were disciplined for complaining about their employer).\footnote{Sprague, Robert. “Facebook meets the NLRB: Employee online communications and unfair labor practices.” University of Pennsylvania Journal of Business Law, Vol. 14, No. 4. 2012 at 957.}

Disciplinary action for protected concerted activity can be a very real risk for workers. About half of large employers use software to analyze the text of employee social media posts, according to a 2018 survey.\footnote{Gartner. “The future of employee monitoring.” May 3, 2019.} One employment service’s background screening of potential employees included scraping social media profiles to determine whether candidates might be potential whistleblowers.\footnote{Bernhardt, Kresge & Suliman 2021 at 9.} Tesla hired a consultant to research its workers’ and especially union organizers’ social media presence to find people that raised unfair labor practices, sexual harassment, or unionization efforts, according to a \textit{CNBC} investigation.\footnote{Kolodny, Lora. "Tesla monitored its employees on Facebook with help of PR firm during 1027 union push," CNBC. June 2, 2022.} The meal kit company HelloFresh used software to mine social media posts on Twitter and Instagram looking for content about unionization efforts and concerns about workplace safety and to identify whether the posts belonged to an employee.\footnote{Kaori Gurley, Lauren. “Internal Slack Show HelloFresh Is Controlling Talk of Unionization,” Vice. November 19, 2021.} Walmart screened its employees’ social media presence to find workers interested in organizing a union.\footnote{Bernhardt, Kresge & Suleiman 2023 at 12.}

\textbf{b. Constant, real-time surveillance causes stress and health harms}

Being surveilled is stressful. Many workers are now under a continuous, real-time, and granular automated worker surveillance that is incredibly stressful. The more powerful, computer-augmented monitoring, tracking, and surveillance affect how workers do their jobs, invade privacy,
and contribute to stress — especially because of accelerated pace and blurred boundaries between work and home.\textsuperscript{115} Algorithmic monitoring for performance has been shown to increase stress, burnout, and contribute to physical health problems.\textsuperscript{116} A 2022 meta-analysis of academic literature found that workplace surveillance increased stress and lowered job satisfaction and that the impact likely led to “severe and aversive consequences for employees’ life and well-being.”\textsuperscript{117}

**Highly-intrusive monitoring of call center agents:** Call centers were among the first adopters of digital surveillance and performance ratings.\textsuperscript{118} Companies monitor call center agents through voice recordings, computer screen shots, keystroke tracking, and reading online chat interactions. Some software monitors calls and offers real-time suggestions to call-center workers to improve their customer interactions and supervisors can monitor a dashboard on each agent that rates their calls.\textsuperscript{119} Most call center workers report at least three types of monitoring, with voice recordings the most common.\textsuperscript{120} The company RemoteDesk offers webcam monitoring of remote call center agents to enforce prohibitions against eating at desks or “detect suspicious gestures.”\textsuperscript{121} Some outsourced, home-based call center workers have been required to install artificial intelligence-enhanced cameras that monitor work in their homes, share biometric data, and submit to polygraphs on demand as a condition of keeping their jobs.\textsuperscript{122}

**Constant surveillance dehumanizes call center workers and leads to higher stress:** The constant monitoring of call center agents and reduced discretion have contributed to higher levels of stress and employee burnout. A 2020 Cornell University study found very high stress levels among 2,000 surveyed call center agents represented by the Communications Workers of America (CWA).\textsuperscript{123} An overwhelming share (87 percent) of workers reported high or very high stress levels among their colleagues and more than three-quarters (77 percent) reported high or very high levels of personal stress, despite finding that the union helped to mitigate the stressful working conditions. More than half the agents had been prescribed medication to treat stress or anxiety disorders and one-fourth were using these medications all the time — far higher rate than a Harvard Medical School study estimate of 19 percent of the population being affected by anxiety disorders.\textsuperscript{124} These call center agent stress levels were associated with increased absenteeism, reduced job satisfaction, and accelerated turnover intentions.

These concerns have risen as more advanced, artificial intelligence-driven call center monitoring and management tools have been deployed. A preliminary 2023 update of the CWA-Cornell survey found that the majority of call center agents were scheduled, assigned calls, monitored, and given feedback on voice tone, pace, and adherence to call scripts by automated systems.\textsuperscript{125} Workers

\begin{itemize}
  \item De Stefano & Taez 2023 at 22 and 27.
  \item Gagné et al. 2022; Ball 2021 at 20.
  \item Simonite, Tom. “This call may be monitored for tone and emotion.” *Wired*. March 19, 2017.
  \item Lippert, Kirchner, & Wiener 2023; Bernhardt, Kresge & Suleiman 2023 at 7.
  \item Doellgast & O’Brady 2020.
  \item Harvard Medical School. *National Comorbidity Survey*. August 21, 2017 at Table 2.
  \item Communication Workers of America communication with the AFL-CIO Technology Institute. June 2023.
\end{itemize}
found the automated feedback and monitoring made their jobs more stressful and higher levels of monitoring were associated with higher job dissatisfaction, absenteeism, and job insecurity. Workers subject to more automated monitoring were also more likely to face discipline and face it unfairly: workers reported that the automated analysis was often faulty or inaccurate and was biased against certain speech styles or dialects that could disproportionately disadvantage call center agents of color.

**Tesla Gigafactory workers under oppressive surveillance:** The workers at Tesla’s autonomous driving software facility in Buffalo, New York are under constant surveillance and performance evaluation that workers report creates an oppressive work environment that leads to constant anxiety and paranoia. Workers are required to use a performance monitoring app that starts with clocking in (but workers can be disciplined for clocking in by app instead of punch clock) and workers are required to be time-on-task for at least 6 hours of every 8-hour shift or face disciplinary action. The facility monitors workers with real-time cameras that cover workstations, hallways, breakrooms, and outdoor areas including picnic tables and the parking lot — only the bathrooms are not monitored by cameras. The camera and computer surveillance system tracks workers’ activity and task performance frame-by-frame that incorporates “quality metrics” that are undisclosed to workers who do not know how to meet Tesla’s workflow expectations. Workers do not know when the workstation cameras are active or which supervisors or what software might monitor the cameras. Workers are assigned tasks almost entirely by app chat networks that can be unclear, requiring workers to chat clarifying guidance that counts against their productivity assessment. Workers must request a “break for technical difficulties” to address chat-related unintelligible or ambiguous task assignments may not be credited by management — increasing their time-off-task, unfairly reducing their productivity score, and potentially facing disciplinary action that can include coaching, improvement plans, or even termination. The surveillance system can fail to accurately measure productivity time-on-task, but workers find it difficult to successfully challenge errors — workers that worry about inaccurate productivity surveillance tracking avoid bathroom breaks when needed to reduce their time-off-task. This oppressive surveillance increases economic and job insecurity for workers that fear unfair and inaccurate digital reprisals. The stress is especially punishing for workers with anxiety-induced mental health conditions or physical conditions like diabetes that need more restroom breaks, who can face additional discipline for delays or declining productivity.

c. Automated surveillance infringes on worker privacy

Technological advances have allowed employers to more intrusively monitor workers’ lives and access and evaluate personal information unrelated to the workplace. Some companies are deploying sophisticated continuous surveillance of credit reports, public records like marital status changes, and “suspicious” computer activity combined with algorithmic sentiment analysis to assess

---

126 Ibid.
127 United Steelworkers communication with AFL-CIO Technology Institute, June 2023.
132 United Steelworkers communication with AFL-CIO Technology Institute, June 2023.
risks to the company that can run from leaking confidential information to worker retention. Digital surveillance has also enabled employers to capture biometric information from workers and track workers outside of work hours.

Several studies have documented how workplace surveillance that undermines privacy — especially social media monitoring, wearable technologies, and location monitoring — can lead to workplace discrimination, unfair dismissals, the erosion of workplace culture and productivity, and gross violations of privacy rights of workers. Most workers have little protection from workplace surveillance. Most workplace monitoring is legal if it is based upon a purported business interest or if it is overseeing company owned equipment (like computer or telephone communications). A spokesperson for the American Management Association stated that “privacy in today’s workplace is largely illusory.”

**Employers track workers’ locations off the job:** Employers have been interested in workers’ home life for ages — Henry Ford sent investigators on home visits to assess employees’ fitness as workers and citizens. Today, employers have a host of tools to monitor workers off the clock, especially location tracking devices and software. Workers rightly view location monitoring or tracking as posing a risk to personal privacy because it can record non-work information. Some employers require workers to download apps onto their mobile phones (both employer-provided and personal mobile phones) that track their movements and geolocation during work hours but also use these apps to monitor workers when they are not on the job.

These geolocation trackers are depressingly common. Walmart workers report being forced to download apps onto their personal mobile phones to scan inventory that also require access to camera and location services to function — unless workers turn this app off after work hours, the software can monitor location and access the camera 24 hours a day. Some families require nannies to use “find-my-nanny” location trackers that monitor domestic workers’ location outside their working hours. Employers can require the use of time-keeping or payroll apps that also always track workers movements. The Washington Post reported that one worker was fired for turning off her location tracking when she was not on the clock despite otherwise exemplary performance. A 2022 list of the best GPS employee tracking apps includes promotional pitches such as “GPS tracking features (that goes with the ability to generate automatic reports about employee locations)” and “app log and updates employee’s location throughout the day.”

---

133 Scholes 2022.
134 United Steelworkers communication with AFL-CIO Technology Institute, June 2023.
135 Sultana & Alam 2022 at 275 to 276.
136 Nguyen 2021 at 29.
139 Ball 2021 at 17.
140 Nguyen 2021 at 12.
141 National Domestic Workers Alliance communication with AFL-CIO Technology Institute, June 2023.
Biometric employee monitoring undermines worker rights and is riddled with bias:
Employers are increasingly requiring workers to submit to biometric monitoring including fingerprinting, facial recognition, retinal scans, heat-mapping, and ergonomic modeling in the workplace. In 2022, truck drivers won a $228 million verdict against railroad company BNSF for requiring workers to confirm load transfers with their fingerprints, in violation of Illinois law.\textsuperscript{145} PetSmart and Whole Foods warehouses settled similar lawsuits under the Illinois biometric privacy law for their use of a headset-based task assignment system that required workers to submit voice samples (so they could communicate with the computer system) — workers were not asked for their consent to provide voiceprints or written disclosure about how the voiceprints would be used, how long they would be kept, or when or if the voiceprints would be deleted.\textsuperscript{146}

Some employers collect health data from employer-sponsored wellness programs that rely on wearable technology like fitness trackers that can be used to monitor heart rates and stress levels and assign unreliable health “risk scores” to their workers.\textsuperscript{147} Amazon has responded to warehouse workplace injuries in part by imposing more intrusive surveillance and “to use sophisticated algorithms to rotate employees among jobs that use different muscle-tendon groups,” but job rotation is not the most effective method to prevent hazards.\textsuperscript{148} Broadly, biometric monitoring does not address or prevent the safety and health hazards that workers face because of their work (for example, Amazon is not proposing to alter the tasks and workload that cause the strains). Facial recognition software is commonly used for contract lawyers and requires teleworking lawyers to confirm their identity for purposes of being able to bill hours. This constant intrusive camera monitoring is demoralizing and excessive.\textsuperscript{149} And since facial recognition has been shown to be racially biased, workers of color had more difficulty being recognized and logging in, thus accruing fewer billable hours than their white counterparts.\textsuperscript{150}

Surveillance data collected from workers commodified by employers: Employers are amassing troves of personal data on workers that is unrelated to their job performance — financial, medical, consumer, and other personal data — and combining it with workplace and worker surveillance tools to create detailed individual profiles of their workers.\textsuperscript{151} But workers have largely been omitted from the growing public discussion about the risks to consumer and personal privacy in an age of ubiquitous digital surveillance and data commodification.\textsuperscript{152} It is harder for workers to protect their data and privacy rights because the privacy risks are imbalanced by the structural power of the employers.\textsuperscript{153} The combination of workplace surveillance and other personal information and data can increase the risk of biased or discriminatory treatment — by employers or other commercial companies — by accessing or determining sensitive information (racial or sexual

\textsuperscript{145} Pierson, Brendan. ”BNSF must pay truck drivers $228 mln for privacy violations.” Reuters. October 13, 2022.
\textsuperscript{146} Bitter, Alex. ”Whole Foods must pay $300,000 over accusations that a system meant to track productivity captured warehouse workers' voices without their consent.” Business Insider. January 26, 2023; Wood, Lauranna. ”PetSmart strikes $425K deal in worker's voice-tracking suit.” Law360. June 9, 2023.
\textsuperscript{148} Ongweso, Edward, Jr. ”Amazon’s new algorithm will set workers’ schedules according to muscle use.” Vice. April 13, 2021.
\textsuperscript{150} Harwell, Drew. ”Contract lawyers face a growing invasion of surveillance programs that monitor their work.” Washington Post. November 11, 2021.
\textsuperscript{151} Bernhardt, Krese & Suliman 2021 at 6; Vitak & Zimmer 2021 at 4; De Stefano & Taes 2023 at 26.
\textsuperscript{152} Nguyen 2021 at 5.
\textsuperscript{153} Cafaliello, Moore & Donoghue 2023 at 3.
For example, women are significantly more likely than men to be concerned about employers viewing them as data subjects.\textsuperscript{154} A 2021 Coworker.org study found that 550 software products used by employers to monitor and manage employees are “collecting and aggregating data about workers at every step of the labor process — hiring/recruitment, workplace safety and productivity, workplace and public benefits, and reskilling/retraining” and were accelerating the commodification of low-wage worker data (which is far more limited and thus more valuable to data brokers).\textsuperscript{155} Workers are concerned that the data collected by their employers can be combined with other personal information for non-work related purposes — and can persist and follow them even when they quit.\textsuperscript{156} The NLRB has warned that “advances in artificial intelligence and algorithm-based decision-making in recent years have made it possible for employers to analyze, sell or otherwise share, and act on the voluminous data that new technologies generate.”\textsuperscript{157} Employers and software vendors that collect this data can sell it into the global data market where it can be matched with other consumer data companies including social media, e-commerce, smartphone apps, internet search where this personal information is further aggregated and commercialized.\textsuperscript{158}

### IV. Automated (or algorithmic) management increasingly controls and harms workers

Employers are increasingly using automated management tools — algorithmic software systems known as algorithmic management — to screen potential job recruits, assign tasks and schedule work shifts, press workers to be more productive, evaluate worker performance, and discipline and terminate workers.\textsuperscript{159} Fundamentally, these systems are about employers exerting control over workers and are associated with workplace injuries, de-skilling, a loss of worker autonomy and dignity, and increased economic insecurity. Workers cannot avoid these workplace harms when these algorithmic management tools are a condition of holding a job.\textsuperscript{160} A 2023 study reported that algorithmic management has become “one of the most disruptive forms of technological change currently being implemented.”\textsuperscript{161}

Automated management is powered by workplace surveillance data to drive the algorithmic and artificial intelligence systems that control workers. The automated worker surveillance and management are interrelated functions that frequently are built into a single system that monitors workers, collects and aggregates data, and uses these data inputs to assign tasks, evaluate workers, and impose discipline.\textsuperscript{162} The employer decides what data is collected, how that data is evaluated

\textsuperscript{154} Zickuhr 2021 at 13.
\textsuperscript{155} Stark, Stanhaus & Anthony 2020 at 1080.
\textsuperscript{156} Negrón 2021 at 6 and 8.
\textsuperscript{157} Nguyen 2021 at 25.
\textsuperscript{158} Abruzzo 2022 at 2.
and weighed, how the data is combined, and how the algorithmic decisions are implemented — whether human managers oversee and/or approve the algorithmic decisions.\textsuperscript{163} Employers are also using algorithmic tools to combine statistical modeling and data mining of workplace and personal data to create predictive assessments of workers’ future behavior, including predicted performance and worker retention.\textsuperscript{164}

Essentially, employers have shifted many formerly human supervisory and management responsibilities to smart algorithms powered by surveillance data that automate managerial tasks, automate workplace decisions, and alter work patterns.\textsuperscript{166} Companies have deployed these systems to oversee large numbers of workers more cheaply than human supervisors.\textsuperscript{167} The employers contend that these systems increase workplace efficiency and productivity, provide meritocratic and objective decision-making, and eliminate dangerous or monotonous jobs.\textsuperscript{168}

But the real purpose of these systems is to tightly control workers. The deployment of algorithmic management cements a power imbalance between employers and workers who do not know how decisions affecting their economic security are being determined.\textsuperscript{169} The AI Now Institute reported that the expansion of algorithmic management “threatens not only to disproportionately displace lower-wage earners, but also to reduce wages, job security, and other protections for those who need it most.”\textsuperscript{170} Women, people of color, and immigrants are more likely to be employed in lower-wage workplaces where they disproportionately suffer the workplace harms of algorithmic management and its potential racial and social biases.\textsuperscript{171}

Algorithmic management has rapidly spread from the platform companies that first used software apps to assign, manage, and pay a large number of dispersed gig workers. Today it is common in brick-and-mortar and remote workplaces.\textsuperscript{172} A 2018 paper by a Carnegie Mellon University researcher reported that “now more than ever, computational algorithms increasingly make decisions that human managers used to make.”\textsuperscript{173} Even before the pandemic, there had been a “rapid acceleration of algorithmic systems that control everything from interviewing and onboarding, to worker productivity, to wage setting and scheduling,” according to a 2019 study.\textsuperscript{174} The pandemic only increased artificial intelligence, machine learning, algorithmic management of remote and hybrid workers.\textsuperscript{175} A 2022 \textit{Canadian Psychology} paper concluded that the “exponential

\textsuperscript{164} Jarrahi et al. 2021 at 3.
\textsuperscript{165} Kinowska & Sienkiewicz 2023 at 26.
\textsuperscript{166} Cafaliello, Moore & Donoghue 2023 at 1; Lippert, Kirchner, & Wiener 2023 at 5282 to 5284; Finnegan, Matthew. (Finnegan 2021). “EU ‘gig worker’ rules look to rein in algorithmic management.” \textit{Computeurworld}, December 15, 2021; Jarrahi et al. 2021 at 2.
\textsuperscript{168} Lee, Min Kyung et al. (Lee et al. 2021). “Participatory Algorithmic Management: Elicitation Methods for Worker Well-Being Models.” Conference Paper, Artificial Intelligence, Ethics and Society Conference. May 19-21, 2021 at 1 and 2; Cafaliello, Moore & Donoghue 2023 at 6; De Stefano & Taes 2023 at 22 and 26; Jarrahi et al. 2021 at 3.
\textsuperscript{169} Barratt, Tom, Alex Veen, and Caleb Goods. “Algorithms workers can’t see are increasingly pulling the management strings.” \textit{The Conversation}. August 23, 2020.
\textsuperscript{170} AI Now Institute 2019 at 10.
\textsuperscript{171} Bernhardt, Krese & Suliman 2021 at 2.
\textsuperscript{172} Lippert, Kirchner, & Wiener 2023 at 5282; Jarrahi et al. 2021 at 2; Fernández-Macias et al. 2023 at 5.
\textsuperscript{173} Lee 2018 at 1.
\textsuperscript{174} AI Now Institute 2019 at 10.
The growth of algorithmic management technological advancements is unparalleled, transforming the world of work in an unprecedented way.176

Employers are now controlling more workers and workplaces through automated systems that are demoralizing, dehumanizing, privacy-eroding, dangerous, potentially discriminatory, and economically destabilizing for workers.

a. Algorithmic management poses risks to workers

Algorithmic management can discriminate against workers, accelerate workloads and contribute to worker safety problems, violate workers’ privacy, harm worker mental well-being, and impose seemingly arbitrary discipline.177 Artificial intelligence-enabled algorithmic management compounds these risks by increasing the unpredictability of decision-making and reducing human oversight of workplace decisions.178

The majority of academic research has found that algorithmic management “generates more negative than positive outcomes for workers” that essentially replaces Taylorism’s tyranny of the clock with the tyranny of algorithm.179 A 2021 literature review of 45 algorithmic management studies found that more than 90 percent of them highlighted the negative impacts on workers, from de-skilling and task variety, lower worker autonomy and increased workplace control, increased work intensity, and job insecurity.180 A Harper’s Magazine investigation concluded that:

Data collection is part of an expensive, high-tech effort to squeeze every last drop of productivity from corporate workforces, an effort that pushes employees to their mental, emotional, and physical limits; claims control over their working and nonworking hours; and compensates them as little as possible, even at the risk of violating labor laws.181

b. Secret and unaccountable algorithmic control harms workers

These “black box” systems are totally opaque to workers and the algorithmic decision-making process is largely unaccountable, meaning workers have little recourse to unfair or biased software decisions. Algorithmic management software systems are unaccountable systems that conceal what data is collected and how the data is used to make decisions.182

The data and the mechanisms for algorithmic management are hidden behind a curtain of trade secrets, proprietary systems, or off-the-shelf software where the employers themselves may not know or understand the data elements considered and weights that determine the algorithmic

---

176 Gagné et al. 2022.
177 Cafaliello, Moore & Donoghue 2023 at 3.
178 Ibid. at 2.
179 Kinowska & Sienkiewicz 2023 at 26.
outcomes. Workers frequently do not know—and employers often do not disclose—whether they are being monitored, what data is collected, and how it is used. The intentional opaqueness of algorithmic systems can maximize employers’ control of workers and workplaces.

The lack of transparency can obscure the harms to workers—problems that grow as algorithmic management systems spread to more employers and occupations. The near total opacity of algorithmic decision-making that governs workplaces can reduce worker autonomy, workers’ ability to make informed choices, and make workers feel subject to unpredictable and inscrutable management decisions. Studies have found strong correlations between the transparency of monitoring systems and workers perceptions of fairness, job satisfaction, and job performance, while more opaque surveillance leads workers to view the monitoring as “purposeless and authoritarian,” according to the European Commission.

Workers have little recourse from the workplace decisions that directly impact their life—discipline, demotions, or terminations—that are based on opaque automated surveillance and automated management systems. Many supervisors cannot or will not review algorithmic decisions because they have no incentive to intervene and could face reprisals for interceding in the employer’s algorithmic management system.

Algorithmic management reinforces management’s power and information asymmetry over workers and the opacity and perceived unfairness of automated decision-making further erodes worker autonomy. The employer’s algorithm knows a lot about the worker, but workers know almost nothing about the system that makes decisions. There is frequently little or no recourse for workers to challenge or dispute the algorithmic decisions or determine what data was the basis for these algorithmic determinations that affect workers.

V. Case studies on the worker harms of algorithmic management

The core algorithmic management functions—hiring, assigning and scheduling, evaluating, and disciplining—have real and overwhelmingly negative impacts on workers. Many workers face overlapping algorithmic management functions that combine to negatively impact them. For example, algorithmic task assignment and productivity evaluations are combined to press workers to toil harder to hit production targets that increase work intensification and can contribute to workplace injuries and stress.

These algorithmic management functions have negative impacts on real workers: recruiting and hiring algorithms can be biased and contribute to employment discrimination; task assignment and

---

183 Hickok & Maslej 2023 at 4.
184 Jarrahi et al. 2021 at 7.
185 Ibid. at 6; Gagné et al. 2022.
186 Ball 2021 at 17.
187 De Stefano & Taes 2023 at 26 to 27.
189 Noponen et al. 2023 at 14.
190 Gagné et al. 2022; Bujold, Parent-Rochelleau & Gaudet 2022 at 4.
productivity monitoring contributes to work intensification that can increase workplace injury risks and rate; task assignment can also lead to de-skill, demoralization, and declining work satisfaction while compromising the quality of services; algorithmic scheduling exacerbates economic precarity for retail and restaurant workers; and algorithmic discipline threatens the economic security of workers and gives them little redress for unfair or biased decisions.

**a. Algorithmic recruiting and hiring tools are riddled with biases that can run afoul of civil rights and employment law**

Employers are using artificial intelligence-driven tools to recruit, screen, rank, and assess candidates’ interview performances which in turn affects prospective workers’ chances of getting hired.\(^{191}\) These tools can include resume screening, emotive response and performance assessments of video interviews, and bots that search candidates’ social media networks that all affect hiring decisions.\(^{192}\) These background checks can be riddled with errors that can wrongly prevent candidates from securing job opportunities.\(^{193}\) This research can screen out politically active and union-sympathetic candidates before they were hired.\(^{194}\) In 2020, more than two-thirds of human resources leaders and recruiters were using artificial intelligence tools to automate recruiting and hiring.\(^{195}\)

These systems can entrench existing subjective preferences that perpetuate racial and social biases that contribute to occupational segregation and racial, gender, and economic inequality.\(^{196}\) The data-driven systems purport to be objective and logical but often have built in biases and rely on faulty data inputs that amplify the detrimental impacts on job applicants.\(^{197}\) Some automated applicant screening processes have made it harder for people with non-white sounding or foreign sounding names, women, older people, or people with disabilities to be interviewed and get a chance at a job.\(^{198}\) As evidence mounts, the discriminatory impact of these artificial intelligence screening and hiring processes are being challenged as potential violations of civil rights and antidiscrimination laws.\(^{199}\)

**b. Task assignment and productivity evaluations lead to harmful work intensification**

Algorithmic systems commonly assign specific tasks to specific workers, directing workers’ activities. Task assignment can be extremely detailed, such as identifying the specific item and its location for warehouse workers to secure for shipment or the specific route a driver must follow. These detailed assignment algorithms are typically paired with performance evaluation tools that

---

\(^{191}\) Yang 2020 at 3 and 4.

\(^{192}\) De Stefano & Taes 2023 at 25; Jarrahi et al. 2021 at 3.

\(^{193}\) Bernhardt, Kresge & Suleiman 2023 at 10.

\(^{194}\) Garden 2018 at 66.


\(^{196}\) Yang 2020 at 4 to 5.

\(^{197}\) Ibid. at 1.

\(^{198}\) Ajunwa 2020 at 5 to 6; Yang 2020 at 4.

impose productivity targets. For example, some logistics employers algorithmically direct workers through headset commands that are tied to activity tracking to assess productivity.\footnote{Ball 2021 at 25.}

Productivity targets can press workers to perform more intensively and contribute to higher workplace injury rates. Performance surveillance includes location monitoring (on shop floors or in delivery vehicles), video monitoring (of worksites or workers), workstation software monitoring (keystroke and mouse tracking), and auditory monitoring (call center workers and retail clerks), and much more. Performance monitoring has been shown to increase stress, burnout, and contribute to physical health problems including repetitive motion injuries and musculoskeletal pain — which are the largest percentage of non-fatal serious workplace injuries.\footnote{Ball 2021 at 26; Gagné et al. 2022; Reindel, Rebecca L. and MK Fletcher. AFL-CIO Safety & Health Department. “Death on the Job: The Toll of Neglect.” April 2023 at 57.} The continuous, real-time surveillance, and constant electronic task assignment can also demoralize, deskill and drain workers.\footnote{Kantor & Sundaram 2022.} They also can worsen economic precarity by affecting pay and promotions, and lead to unfair discipline — even firings for failing to hit performance targets. A 2023 *European Labour Law Journal* concluded that algorithmic management “poses significant occupational safety and health risks for workers.”\footnote{Kantor & Sundaram 2022.}

Performance evaluation systems measure the number, difficulty, and accuracy of the tasks workers perform and if worker performance lags, they can be nudged to work harder, disciplined, or even fired.\footnote{Cafaliello, Moore & Donoghue 2023 at 1.} “These systems rely on granular surveillance data to measure time-on-task, customer service behaviors, location tracking, and other metrics for worker effort and performance.”\footnote{Bernhardt, Kresge & Suleiman 2023 at 8 to 9.} Systems evaluate, rate, rank, and compare workers performance in real time.\footnote{Kinowska & Sienkiewicz 2023 at 26.}

These worker productivity ratings and evaluations can affect workers’ income but can be based on inaccurate information, faulty equipment, imperfect proxies for performance, and present a distorted picture of workers’ activities and effectiveness.\footnote{Gagné et al. 2022.} These systems do not actually promote more productivity or better performance. A 2022 meta-analysis of over 60 studies found no association between electronic monitoring designed to increase productivity and job performance and concluded that “there is most probably no overall effect of electronic monitoring on performance.”\footnote{Kantor and Sundaram. August 14, 2022; De Stefano & Tacs 2023 at 25.} Workers cannot contest unfair or biased decisions that impact their job and economic security when they cannot access or challenge the underlying data, assumptions, or automated decisions of non-transparent algorithmic management systems.

**Amazon warehouse algorithmic task assignment and productivity evaluations associated with higher rates of workplace injuries:** A particularly striking example of algorithmic management leading to workplace injuries is provided by our country’s second-largest employer: Amazon. The company’s warehouse workers are monitored by artificial intelligence-enhanced security cameras and handheld package scanners that track worker movements and evaluate work speed, and Amazon even terminates workers based on data collected on workplace productivity.\footnote{Siegel, König & Lazar 2022 at 8.}
metrics. Amazon tracks every minute workers are “time-off-task” through their handheld devices, and if workers accumulate 30 minutes of time-off-task on three days over a year (or 120 minutes in a single shift), they are fired. Amazon managers are further directed to discipline the worker with the most time-off-task every shift.

The European Commission described digitally surveilled and managed workers at Amazon warehouses as toiling “amid a culture of fear.” Workers believe that maintaining a high package pick rate is essential to getting permanent or better positions, creating strong incentives to increase work intensity. Workers have been disciplined and even fired for failing to hit pick-rate productivity targets. A 2020 study found that Amazon’s warehouse worker productivity programs have ratcheted up workloads and work speed and contributed to the company’s sky-high serious injury rate. A 2022 Strategic Organizing Center study found that the during the pandemic, the number of Amazon’s warehouse injuries rose 20 percent from 2021 to 2022, the serious injury rate was double the national average for warehouses, and that although Amazon employed one-third of the national warehouse workers, it was responsible for half of the warehouse injuries in 2021.

Task management apps intensify hotel housekeeper work and increase risk of injury: The hospitality industry has widely adopted algorithmic management tools across hotel operations, including chatbots, mobile check-in, and devices to assign and manage employee tasks, impacting the industry’s frontline workers who are predominantly women, people of color, and immigrants. Hotel housekeepers have some of the highest hospitality industry injury rates from pushing hundred-pound carts, scrubbing floors, making dozens of beds, and other physically demanding work. Many hotel companies use apps that direct housekeeper work by assigning the sequence of rooms for workers to clean. The apps can direct workers to spend time moving from floor-to-floor, inefficiently ignoring nearby dirty rooms and leaving workers worried they would be disciplined for not completing their tasks. The apps also sometimes forces workers to clean multiple, more intensive, check-out rooms in a row, rather than allowing housekeepers to switch between check-out and stayover rooms to pace their workload, as they had typically done before the advent of the apps. The apps can incentivize workers to speed up in order to meet their daily room quotas while following the algorithmic management that might direct them to move between floors or distant hotel wings, or to over-exert themselves by cleaning multiple check-out rooms, potentially increasing the likelihood of an injury. The apps can have the incidental impact of reducing the

---

209 Constantz 2021; Wood 2021 at 8 to 9.  
211 Ibid.  
212 Ball 2021 at 12.  
213 Wood 2021 at 7.  
personal service housekeepers provide to longer-term guests, diminishing quality service and reducing job satisfaction for the housekeeper.\textsuperscript{221}

**Telemetric surveillance of delivery and long-haul drivers intensifies workloads:** Employers track long-haul truck drivers and local delivery drivers by cameras, biometric monitoring, motion and equipment sensors that manage and control these workers.\textsuperscript{222} Trucking companies can monitor, supervise, and evaluate long-haul drivers remotely by monitoring real time geolocation, speed, braking, acceleration, fuel use, and cargo status (pick-ups, departures, and even temperature).\textsuperscript{222} UPS installed over 200 sensors on its delivery trucks to track deliveries, drop-off times, operating efficiencies, driver speeds, and more that is transmitted in real time to supervisors; this has increased deliveries while slashing 22,000 jobs, leaving remaining workers pressed to work harder and faster under surveillance one driver called a “mental whip.”\textsuperscript{224}

c. **Task assignment leads to deskilling and undermines quality**

Algorithmic task assignment can dehumanize, deskill, and demoralize workers. It also frequently reduces the quality of service when workers’ learned, on-the-job expertise is overruled by algorithms that assign tasks and minutely direct workers’ activities. The algorithmic management systems emphasize and reward workers’ completion of specific assigned tasks, which ultimately shunts workers to less skilled, fulfilling, and remunerative jobs.\textsuperscript{225} These systems encourage human managers to view workers as fungible cogs in the workplace rather than human beings employed by the company.\textsuperscript{226}

As algorithmic tools take over decision-making tasks, workers’ acquired skills become less valuable and, unless they are upskilled in other areas, suppresses earnings and wage growth and demeans the dignity of their occupations.\textsuperscript{227} This has de-skilled the workforce by reducing the skill set required, the wages paid, and worker autonomy, job satisfaction, and dignity.\textsuperscript{228} A 2023 survey of nearly 22,000 European human resources professionals found that algorithmic management was associated with a decline in worker well-being — including workers’ sense of self-worth and job satisfaction.

**Home healthcare workers deskilled, short-changed on wages, and discourage social caregiving:** Home healthcare workers can have their caseload driven by algorithms that raise the number of assigned patients, grade workers on the number of specific procedures or actions, and discourage social caregiving time in order for workers to receive better scores and benefits like pay or schedule improvements.\textsuperscript{229} Home care companies assign home care worker resident visits that are governed by Medicaid-required electronic visit verification (EVV) systems that can require

\textsuperscript{221} Spektor et al. 2023 at 208.
\textsuperscript{223} Bujold, Parent-Rocheleau & Gaudet 2022 at 1 to 2.
\textsuperscript{224} Kaplap 2015.
\textsuperscript{225} Jarrahi et al. 2021 at 6.
\textsuperscript{226} Ibid. at 4.
\textsuperscript{227} Cafaliello, Moore & Donoghue 2023 at 6.
\textsuperscript{228} Nunes, Ashley. “Automation doesn’t just create or destroy jobs—it transforms them,” Harvard Business Review, November 2, 2021.
\textsuperscript{229} Kinowska & Sienkiewicz 2023 at 34.
workers to enter visit data into a portal, download a smartphone geolocation and visit tracking app, and a few states require biometric facial or voice recognition of the worker and the home care recipient. Electronically logging and documenting each task can interfere with providing care in real life. The focus on performing and reporting specific tasks (like bathing or eating) leaves workers in a bind about either ignoring the human component of their job or underreporting their hours.

Home health workers report that the apps often do not function well and either underreport work time, resulting in wage theft, or force workers to spend time submitting app check-ins when they should be tending to recipients. The EVV apps can also compromise the privacy of workers (who may use their personal device to log hours and be subject to GPS tracking) and home care recipients (who worry that the data collected will be captured and sold or shared and could be used to deny future eligibility or benefits).

These algorithmic task assignment problems are not unique to home health workers in the United States. A survey of algorithmic surveillance and management of home care workers in the United Kingdom found that the workers felt distrusted and the time-management software discouraged relational companionship with their patients that degraded their work and undermined their autonomy and discretion to care for their patients.

Algorithmic task assignment and productivity quotas overburden public employees and compromise service to the public: Federal government automated task assignment and productivity quotas can discourage public employees from more considered evaluation of complex compliance, fact-finding, and administrative adjudication proceedings that can overburden workers, undermine the delivery of quality public services, diminish fairness and due process, and compromise ethics and accountability in government administration.

The imposition of time-based, performance-linked metrics on union members represented by the International Federation of Professional and Technical Engineers (IFPTE) who preside over administrative adjudication proceedings at the Social Security Administration (SSA) and the Department of Justice’s Executive Office of Immigration Review’s (EOIR) Immigration Court report that these production quotas amount to a line speed-up. This productivity monitoring undermines independent decision-making, impartiality, and due process and creates a tension between adjudications based on their circumstances and hitting case quotas that affect their performance appraisals.

A 2021 Government Accountability Office study found that SSA did not give administrative law judges sufficient time to perform conscientious disability eligibility reviews and that the agency
never documented a rationale for its caseload quota.\textsuperscript{237} SSA’s training modules promote more deliberative decision-making to reduce potential racial bias and provide full and fair hearings for claimants.\textsuperscript{238} The Trump administration’s digital performance dashboard metric for immigration judges emphasized case quotas and time-based deadlines over judicial competence and were unattainable targets for almost all judges.\textsuperscript{239} The Biden administration has rolled back most of the problematic measures but maintained the dashboard to assess performance based on the Trump-era metrics.\textsuperscript{240}

The lack of transparency on how data is used to assess caseload and performance and the failure to engage with the employee unions has harmed morale and raised deskill concerns. The algorithmic task assignment and performance quotas disregard adjudicator expertise, diminish their independent judgment, and fail to provide the necessary information for these employees to perform their public service jobs and duties.

**Automated public benefits and social services task administration can deskill workers and deny benefits that can be biased and erroneous:** Public agencies have been deploying algorithmic systems to collect and assess information on people interacting with social service agencies that purport to make more efficient and objective determinations that can deeply affect people’s lives.\textsuperscript{241} These systems circumvent the subtle assessments of social workers and case managers that can take individual cases, context, and situation into account. These algorithmic systems can incorrectly deny eligibility or reduce benefits in an opaque and unaccountable manner that raise concerns about what data elements the algorithm considers, how it evaluates these elements, and how eligibility or benefits are determined.

A 2022 study of algorithmic child welfare systems that are tasked with making critical determinations to protect children from harm reported that most automated systems were driven by a risk-based model that was racially biased and failed to account for complexities and uncertainties in casework that undermined caseworker autonomy and discretion.\textsuperscript{242} A 2018 survey and focus group of child welfare caseworkers, families, and experts in the United States found broad distrust of algorithmic decision-making, frustration with the opaque determinations, deep concerns with potential bias and discrimination based on race, ethnicity, gender, economic status, and geography, and workers felt that their expertise and experience were discounted.\textsuperscript{243}

These algorithmic determinations can inappropriately or erroneously deny benefits or pursue and punish eligible recipients for fraud incorrectly — in some cases, based on discriminatory algorithmic decisions. In Idaho, people with disabilities successfully sued when an automated


\textsuperscript{238} International Federation of Professional and Technical Employees communication with AFL-CIO Technology Institute. June 2023.


\textsuperscript{242} Ibid.

system cut community-based care reimbursements below the expenses for about 15 percent of recipients without disclosing the rationale for the reductions, making it hard for people with disabilities to redress these determinations.\footnote{KW v. Armstrong 180 F. Supp. 3d 703 — Dist. Court. Idaho 2016.}

Australia’s algorithmic welfare overpayment enforcement system imposed “robodebt” penalties on 70,000 people accused of receiving payments because the system incorrectly over-assessed their incomes.\footnote{Henriques-Gomes, Luke. “Centrelink cancels 40,000 robodebts, new figures reveal.” The Guardian. February 5, 2019.} In the Netherlands, a tax authority’s anti-fraud AI algorithm incorrectly accused families of illegally receiving publicly-funded childcare that targeted “non-western” appearing families, especially those with Turkish or Moroccan backgrounds.\footnote{Heikkla, Melissa. “Dutch scandal serves as a warning for Europe over risks of using algorithms.” Politico. March 29, 2022; Henley, Jon “Dutch government faces collapse over child benefits scandal.” The Guardian, January 14, 2022; Biedermann, Ferry. “Victims of Dutch childcare benefits scandal struggle to move on.” Thomson Reuters Foundation. March 17, 2022.} Over six years, more than 20,000 families were wrongly charged with fraud, pursued for repayment, blacklisted as fraudsters, and denied the right to appeal the rulings — many families went into bankruptcy trying to repay benefits to which they were eligible.\footnote{Ibid.} The tax authority was ultimately required to pay €6.5 million in fines for the erroneous and biased algorithmic mistreatment.\footnote{Ibid.}

**Parole risk assessment algorithms deskill and overwork parole officers and jeopardize community safety:** State and local governments are using risk-assessment algorithms to determine bail, sentencing, prison management and parole.\footnote{Electronic Privacy Information Center. “AI in the Criminal Justice System.” Accessed June 2023.} These systems replace the judgment of seasoned parole officers in making complex decisions that balance the potential for individual rehabilitation with the potential risks to community safety. Faulty and biased risk assessments can endanger community safety, exacerbate racial disparities, and erode working conditions for parole officers that may have higher caseloads and misleading risk-profiles for those in their charge. New York state uses the widely-used Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) to make parole supervision decisions.\footnote{Angwin, Julia et al. (Angwin et al. 2016). “Machine bias: There’s software used across the country to predict future criminals. And its biased against Blacks.” ProPublica. May 23, 2016.} The COMPAS program requires parole officers to administer a questionnaire that relies on parolees’ truthful answers to generate a risk score.\footnote{COMPAS, “Risk Assessment.” 2011.} Researchers have found that the COMPAS assessments were tainted with potential racial bias, were a “remarkably” poor predictor of future violent crimes, and were only slightly better than a coin toss at predicting any non-violent violations, including misdemeanors.\footnote{Angwin et al. 2016; Dressel, Julia, and Hany Farid. “The accuracy, fairness, and limits of predicting recidivism.” ScienceAdvances. January 2018.}

The COMPAS system disregards parole officers’ professional judgment and contextual knowledge of individual cases and can lead to inaccurate risk assessments and inappropriate supervision levels. The state parole department has implemented the automated COMPAS system to justify understaffing and increasing caseloads, which heightens parole officer stress and exhaustion. The New York Public Employee Federation that represents parole officers surveyed its membership and found that 73 percent reported that COMPAS’ assigned supervision level rarely reflected the actual risk level posed by parolees, 83 percent reported that COMPAS is not collecting the
information it needs to accurately assess parolee supervision levels, and 63 percent reported
COMPAS had a negative impact on their work.\footnote{Elish, Madeline Claire and Elizabeth Anne Watkins. Data & Society. "Repairing Innovation: A Study of Integrating AI in Clinical Care." September 2020.}

**Algorithmic task management of nursing can deskill workers and reinforce biases:** A pilot program that used artificial intelligence to identify hospital patients susceptible to the dangerous infection sepsis required nurses to develop new skilled approaches to navigate professional hierarchies, implement new workaround procedures, and other social skills to help physicians act on the new infection-monitoring technology.\footnote{Berridge, Clara and Alisa Grigorovich. "Algorithmic harms and digital ageism in the use of surveillance technologies in nursing homes." Frontiers in Sociology. September 16, 2022.} Algorithmic surveillance and management in nursing homes includes real-time location, fall detection, activity sensors, electronic medical records, and automated and predictive care decision-making that tends to reinforce control and power structures that amplify bias against older and disabled residents and controls and disciplines the low-paid Black, Latinx, and immigrant women that make up the majority of the workforce.\footnote{Gagné et al. 2022.}

**d. Scheduling algorithms and performance evaluations exacerbate economic precarity**

Algorithmic scheduling software is designed to manage large workforces in multiple locations, but these systems are designed for the employer to minimize labor costs and workers often face uncertain, rapidly changing schedules that worsen their economic precarity and work-life balance.\footnote{Jarrahi et al. 2021 at 3; Greenhouse, Steven. (Greenhouse 2012). “A part-time life, as hours shrink and shift.” New York Times. October 27, 2012.} These systems typically try to reduce labor costs by matching the retail, restaurant or other service sector workforce to anticipated customer demand based on sales data, seasonal shopping traffic, and even the weather.\footnote{Gagné et al. 2022.} Some software tools break shifts into 15-minute increments and cancel or extend shifts with less than 24-hour’s notice to workers to closely match customer traffic that can cut corporate labor costs by up to 5 percent while upending the economic fortunes of workers that cannot secure enough hours.\footnote{Rogers 2023 at 76.}

These systems can account for workers’ shift preferences and availability, but the primary goal is to match the workforce to anticipated customer demand.\footnote{Kaplak 2015.} Automated scheduling software can contribute to wage theft — failing to fully pay workers for all the time worked under wage and hour laws — because the software can undercount hours and allow employers to edit and reduce the number of recorded hours worked.\footnote{Rogers 2023 at 76.} Algorithmic scheduling software can also deduct unpaid breaks that were never taken or misattribute paid sick leave or managers can press workers to clock out but keep working to hit productivity targets that amount to highly profitable wage theft.\footnote{Rogers 2023 at 76.}

**Algorithmic scheduling exacerbates the economic precarity of low-wage retail workers, who are predominantly women and people of color:** Retail companies use algorithms to
automate just-in-time shift schedules to minimize operating costs that often leave workers without stable work schedules that reduce economic stability and disrupt family life. For example, the Dollar General chain automates scheduling for 16,000 stores to match customer forecasts. Retail workers under algorithmic scheduling get shorter hours (4 hour shifts or 12 hour weeks), on-call shifts that never deliver actual work, and shift assignments without prior notice, thus converting full-time jobs into part-time jobs that are more akin to day laborer pick-up jobs. One retailer adopted algorithmic scheduling software that converted hundreds of full-time workers into part-time workers, making them ineligible for health benefits.

Algorithmic scheduling contributes to the economic precarity of retail workers. Half of retail workers face uncertain scheduling that compounds the economic precarity that they face from low wages. These erratic schedules harm people of color and women that make up the majority of the low-wage retail workforce that already face enormous economic hardship. Over three-quarters of retail workers are low-wage earners receiving only about $10 an hour. Women make up more than half the retail workforce but earn less than their male colleagues, fill three-quarters of the lowest-wage cashier positions, and are far less likely to be supervisors. Black and Latinx workers constitute a big portion of retail workers (12.5 percent and 18.7 percent, respectively), and they are concentrated in cashier jobs. Because of this occupational segregation, over 40 percent of Black and Latinx retail workers have incomes putting them near or below the poverty line.

**Scheduling software and performance monitoring worsen the economic precarity of restaurant workers:** Many chain restaurants have adopted a tablet-based ordering and waitstaff rating system that management has used to assign tables and shifts — punishing workers who receive low customer ratings by cutting the number of hours, reducing prime shift times, or reducing the number of tables in their sections, substantially reducing their earnings. These reviews can include factors beyond a server’s control — like food quality or restaurant atmosphere — that nonetheless can undermine their economic security.

e. **Algorithmic performance evaluation and discipline unfairly and unaccountably stigmatize and threaten workers livelihoods**

Many algorithmic management systems can discipline or fire workers for failing to achieve productivity or performance metrics. Some algorithmic systems encourage workers to hit higher

---

263 Gagné et al. 2022.
264 Kaplan 2015.
269 Ibid.
272 Nguyen 2021 at 13.
productivity targets with bonuses for exceeding specific targets or outperforming coworkers in gamified workplace contests. Many performance monitoring systems score workers on efficiency or productivity based on worker activity and managers use the scores to discipline or reward workers. Workers even can be fired by algorithmic systems without the involvement of a supervisor, a practice most common in platform work but has also occurred at Amazon warehouses.

Workers who know that they can be abruptly disciplined or even fired for failing to hit algorithmic evaluative targets face heightened anxiety over potential job loss. A 2023 survey found that almost all (98 percent) human resources leaders admitted that they intended to use algorithms to select which workers would be fired, especially to deal with the thousands or tens of thousands of layoffs sweeping the tech sector.

Teachers have been evaluated on how students performed on standardized tests compared to their expected performance based on predictive computer analytics. Teachers can be rewarded, disciplined, and even fired based on proprietary algorithmic assessments that could be based on incorrect data points (classes teachers had not taught) or software code glitches — decisions that school administrators cannot explain or justify, because even they do not know how the systems work. An algorithmic management and discipline program controlling small rural post offices in the United Kingdom wrongly identified 700 postal workers as committing theft and the workers began facing criminal charges before the software error was unraveled.

Office workers subject to growing electronic monitoring and discipline: The pandemic hastened the shift of office workers to a platform-based management system where employers use networked systems and software to control workflows, employee communication and collaboration, monitor workers, evaluate performance, and impose discipline. This can harm the more than 40 percent of union members who are in professional, technical, and office occupations. This surveillance has become more common since the pandemic increased the number of teleworkers, and employers have increasingly uses productivity metrics to discipline and terminate remote workers. Employer interest in monitoring software had risen over 80 percent from 2020 to 2022.

Software packages like Microsoft Teams can assess individual workers’ productivity, work patterns, activity, interactions as well as organizational trends across the same sorts of metrics. Some surveillance software claims to take 20 computer screenshots per minute, evaluate productivity,
and monitor unspecified high-risk activity. Some companies have activated teleworkers’ microphones to listen to workers remotely. Employers and managers can monitor office employees through network-connected applications (Zoom, Slack, Microsoft Office, Google Workspace).

Employers purportedly implemented many of these software surveillance tools to manage work time, but in practice they are used to evaluate productivity through near-continuous monitoring. The majority of computer monitoring software is capable of being concealed from workers that is “indistinguishable from stalkerware,” according to the Electronic Frontier Foundation, and many employers require workers to reconfigure their antivirus software to keep these monitoring tools undetectable.

Most of these productivity assessments track mouse movements and keystrokes, but not actual effectiveness. Management software scored office workers’ productivity based on email responsiveness, application usage, coworker interactivity, mouse clicks, and keyboard activity. One common office productivity metric is whether a worker’s keyboard or mouse is “idle” for more than 15 seconds. Evaluating employees based on activity is “arbitrary” and “usually counterproductive,” according to a Slack vice president. Despite the flaws in office performance evaluation, a 2022 Digital.com survey found that 60 percent of companies that allowed remote work have deployed monitoring software to monitor workers and 88 percent of those companies that had utilized such software had terminated workers based on information from the surveillance software.

**Algorithmic management and discipline of gig workers suppresses earnings:** Platform company algorithms assign tasks (or gigs), rate and evaluate worker performance, determine pay for tasks, and discipline or deactivate workers which undermines gig workers earnings and forces workers to toil long hours to make ends meet. Algorithmic management of gig workers too often erodes workers’ economic security by assigning tasks or suppressing earnings through pricing algorithms that can overwork and underpay gig workers. A 2017 study by University of Oxford researchers concluded that although gig workers were promised flexibility and autonomy, algorithmic management “mechanisms of control can also result in low pay, social isolation, working unsocial and irregular hours, overwork, sleep deprivation and exhaustion.”

Gig workers are disproportionately people of color, immigrants, and lower-income, meaning the exploitative and unfair algorithmic terms of their work exacerbate racial and economic inequalities. Gig drivers are often paid under algorithmic rates that use secret calculations to set...
fares and charges that have tended to lower earnings — and enable the platform companies to figure out the low range of pay drivers might accept.\textsuperscript{293} The Washington Post reported that changes to pay rate algorithms pushed earnings down by as much as 50 percent for the same number of hours and trips.\textsuperscript{294} Some delivery platform companies may have allowed the pay algorithm to siphon customer tips from drivers, amounting to digital wage theft.\textsuperscript{295} In 2020, delivery workers for Shipt collaborated on independently collecting their own gig pay rates and determined the company’s new and purportedly fairer pay algorithm ended up imposing a 40 percent pay cut on drivers.\textsuperscript{296}

Platform companies also use algorithms to discipline or block gig workers from jobs. Algorithms can wrongly downgrade workers for fraudulent activity or suspend their accounts without disclosing the alleged misdeeds or providing a remedy.\textsuperscript{297} These platform “deactivations” amount to short-term furloughs by algorithms that reduce earnings.\textsuperscript{298} The combination of platform algorithmic evaluation and discipline pushes workers to work intensively for long hours without a break.\textsuperscript{299} Uber drivers have claimed that the company’s driver rating system by passengers is racially biased and is more likely to deactivate or terminate drivers of color.\textsuperscript{300}

**VI. Collective bargaining over automated workplace surveillance and management technologies should be widely encouraged**

Collective bargaining is the best way for workers to protect against the harms of algorithmic management, digital surveillance, and automated decision-making in the workplace.\textsuperscript{302} Collective bargaining empowers workers to speak out and negotiate over the harmful technologies that employers have been seeking to adopt without worker knowledge, input, or consent. In addition, given the rapid pace of technological change, collective bargaining provides a mechanism to help ensure that worker protections evolve alongside technological change and workers are upskilled into new technological implementations.

To date, most bargaining has been over the effects of technologies (the impacts on job security or benefits) but not bargaining over the adoption of worker-assistive (not replacement) technologies — what technology, the manner it is implemented, how it is used, and who has control over the data. Labor unions successfully addressed informational asymmetry under scientific management of Taylorism in the mid-20\textsuperscript{th} century by bargaining for access to the data companies used to set wage rates and workplace conditions, critiquing and challenging the company studies that set wages, and

\textsuperscript{295} Calacci & Pentland 2022 at 428:1.
\textsuperscript{296} Ibid. at 428:2.
\textsuperscript{298} Kaori Gurley, Lauren. “Workers need to unionize to protect themselves from algorithmic bosses.” Vice. December 19, 2019.
\textsuperscript{299} Wood 2021 at 10.
\textsuperscript{300} Allyn, Bobby. “Uber fires drivers based on ‘racially biased’ star rating system, lawsuit claims.” NPR. October 26, 2020; Wiessner, Daniel. “U.S. agency says Uber should face claims that driver ratings are biased.” Reuters. April 3, 2023.
\textsuperscript{301} De Stefano & Taes 2023 at 27 and 29.
selectively participating in workplace decision-making, including in developing time studies; unions can and should bring these kinds of strategies into the digital age.\textsuperscript{303}

Workers represented by a union have some protections from workplace surveillance because employers are supposed to notify and bargain with unions \textit{before} surveillance systems are put in place. In 1996, the National Labor Relations Board ruled that Colgate-Palmolive’s deployment of hidden surveillance cameras violated workers privacy, affected the workplace and workers, was not within the company’s managerial discretion, and the union had a right to have the monitoring disclosed and to bargain over the imposition of the surveillance.\textsuperscript{304} In 2004, the NLRB found that Anheuser Busch violated the National Labor Relations Act when it installed hidden cameras in work and break areas without notice and bargaining with the union.\textsuperscript{305}

Unions are bargaining over the development and deployment of technology. Teachers unions promptly negotiated memoranda of understanding with school districts at the beginning of the pandemic to ensure that the shift to virtual learning could occur rapidly, that it supported student learning, and would not harm teachers.\textsuperscript{306} For example, many agreements protected teachers from disciplinary action when technological hiccups beyond the teacher’s control interrupted virtual learning.\textsuperscript{307} The Screen Actors Guild-American Federation of Television and Radio Artists (SAG-AFTRA) has negotiated, and continues to negotiate across all areas of its jurisdiction, protections for creative artists from artificial intelligence deepfake expropriation of their image, likeness, or voice without explicit prior consent and compensation.\textsuperscript{308} It is also working on federal legislation to protect against voice and likeness replica misappropriation in expressive works.

Beginning in 2018 and 2019, UNITE HERE, the largest U.S. hospitality workers’ union representing nearly 300,000 workers, secured agreements with hotel, casino, and food service employers that require advanced notification and negotiation over the implementation of new technologies.\textsuperscript{309} The Las Vegas–based UNITE HERE affiliated Culinary Union secretary-treasurer Geoconda Argüello-Kline stated that the Las Vegas version of the agreements included “innovative automation and technology language, which set clear goals for worker retention, job training, advance notice of implementation, and severance package based on years of service if workers are laid off.”\textsuperscript{310} In recent years, UNITE HERE has also negotiated to ensure that hotel housekeepers have GPS-enabled panic buttons to alert hotel security if they feel unsafe or threatened, a not uncommon occurrence for housekeepers who have faced sexual harassment and assault from hotel guests.\textsuperscript{311}

\textsuperscript{303} Calacci & Pentland 2022 at 428:5; Lee et al. 2021 at 2.

\textsuperscript{304} National Labor Relations Board (NLRB). Colgate-Palmolive Co. 323 NLRB 515. 1997.

\textsuperscript{305} NLRB. Anheuser Busch, Inc. 342 NLRB 560. 2004.


\textsuperscript{307} Memorandum of Understanding between District of Columbia Public Schools and Washington Teachers Union, Local #6 American Federation of Teachers, AFL-CIO. August 18, 2021 at 2.


\textsuperscript{310} O’Connor, Devin. “MGM Resorts might replace certain jobs with automated technologies.” \textit{Casino.org}. March 6, 2019.

\textsuperscript{311} Snicketo et al. 2023 at 20:9 to 20:10; Gray, Katurah and Lauren Effron. “Hotel housekeepers use panic buttons to feel safe on the job.” \textit{ABC News}. April 20, 2018.
The International Federation of Professional and Technical Engineers’ members who are Administrative Law Judges are subject to automated surveillance and data collection that has negative impacts on morale, engagement, and public service, including cameras in non-public hearing rooms and surveillance of office software, applications, and telecommunications. The IFPTE has negotiated to prevent accessing computer webcams without prior written authorization unless it is during a public hearing or training and requires the Social Security Administration to provide advance opportunity to negotiate over any changes to recording policy during hearings.\textsuperscript{312}

Workers and unions must have a meaningful voice in the development and deployment of technologies that impact the quality and security of more and more jobs.

\textbf{VII. Conclusion and recommendations}

The OSTP should pursue an all-of-government approach to build strong guardrails and safeguards to protect workers from the negative impacts of automated workplace surveillance and algorithmic management. The United States has a patchwork of largely outdated statutes and regulations that fail to protect workers from the potential abuses of the digital world.\textsuperscript{313} For example, federal laws protecting personal data cover some specific areas (like medical information, credit, or financial data), but do not require companies to notify or compensate people if their personal information is shared or sold or exposed to unauthorized parties through cybercrime or data breaches.\textsuperscript{314}

There are effectively no regulations overseeing the impact of algorithmic management and workers have little protection or recourse from digital surveillance on or even off the job.\textsuperscript{315} The existing workplace standards such as workplace safety, wage and hour rules, the right to form unions, and privacy protections do not fully confront the risks posed by algorithmic management in today’s workplaces.\textsuperscript{316}

The OSTP should pursue efforts to apply existing labor and employment law in the new digital environment but also set a robust regulatory and procurement agenda to confront the emerging risks that workers face from automated surveillance and algorithmic management. That should include making sure that regulatory approaches that address algorithmic and artificial intelligence technologies include workers in the highest level of protection, similar to the European Union’s coverage of workers in its high-risk category for workplace deployment of artificial intelligence.\textsuperscript{317}

Other areas for consideration should include:

\textit{The administration must protect workers’ rights to form and join unions and encourage collective bargaining over surveillance and management technologies:} Employers use advanced digital software powered by artificial intelligence to surveil workers and interfere with, restrain, or coerce employees in the exercise of their right to engage in union activity and/or other protected concerted activity. The NLRB has issued a memo on how automated surveillance can

\footnotesize{\textsuperscript{312} International Federation of Professional and Technical Engineers with AFL-CIO Technology Institute. June 2023.} \textsuperscript{313} Kerry, Cameron F. Brookings Institute. “Why Protecting Privacy is a Losing Game Today—and How to Change the Game.” July 12, 2018. \textsuperscript{314} Klosowski 2021. \textsuperscript{315} Bernhardt, Kresge & Suliman 2021 at 2; Ajunwa, Crawford & Schultz 2017 at 738 to 739. \textsuperscript{316} Cafaliello, Moore & Donoghue 2023 at 2. \textsuperscript{317} De Stefano & Taes 2023 at 31.
violate workers’ rights and the administration must rigorously pursue cases against employers using these tactics that violate the National Labor Relations Act. In addition, employers should be required to bargain in good faith with unions over the adoption and impact of automated workplace surveillance and management technologies, as the National Labor Relations Act requires.

The administration should vigorously pursue enforcement of current labor law against emerging algorithmic negative impacts on workers: Algorithmic management has been demonstrated to undermine labor and employment law. Productivity algorithms that prod employees to work harder are associated with higher workplace injury rates, algorithmic just-in-time scheduling has led to management forcing people to work off the clock or skip breaks in violation of wage-and-hour law, and artificial intelligence-powered hiring software has been demonstrated to discriminate against workers of color, women, non-native workers, and people with disabilities. The administration should uphold current labor and employment law even — and especially — in the new digital environment.

The administration should require employers to disclose digital surveillance: Workers should know whether they are being surveilled on the job. The Department of Labor and the Federal Trade Commission should require employers to disclose all workplace surveillance — before it is deployed and/or before workers are hired. That includes how surveillance is performed, what specific data is collected, the purpose for the surveillance, when data is being monitored, how long data is retained, who gets access to the data, how this information is used, whether the employer sells or aggregates the data with other personal information, what rights workers have over personal information or data collected or assembled by their employer, and the right to remedy errors in their personal information and data collected by the employer.

The administration should require employers to get workers’ input and consent before deploying algorithmic management: The current deployment of algorithmic management has demonstrably harmed workers’ physical and emotional health, economic security, and worker autonomy and job satisfaction. Participatory development of algorithmic workplace tools that involve workers pre-deployment can help workers express preferences about technology configurations or how the software can best work to achieve the employer’s goals and take worker well-being into account. The OSTP should re-emphasize the right of labor unions to negotiate over worker surveillance and algorithmic management as the technologies are developed, before they are implemented, and after they are deployed.

The administration should require employers to minimize data collection on workers and provide workers with data privacy and data disclosure rights: Employers should not be able to collect an unlimited amount of data on workers, use it for their own purposes, and hold it forever. The administration should pursue data minimization principles for all automated worker surveillance, algorithmic management, and artificial intelligence applications that affect workers that limit data collection to the data elements that are directly relevant, that are necessary for a legal purpose, and maintain data for limited time. Workers should have a right to know what data is collected, how it is collected, where it is collected, when it is collected, who has access to the data,

---

1 Spektor et al. 2023 at 20:12.
the right to review the data and remedy any errors, and the right to redress in the event of data breach or other privacy infringement.

**The administration should protect workers from the commodification of personal data collected from workplace or other employer surveillance:** The federal government should ensure that workers, not employers, control the data that is collected about themselves — whether it is personally identifiable or whether it is stripped of identifying content. Employers should not be able to share, sell, aggregate, process, or transfer data or information collected about an employee without their express consent. The consent to share, transmit, aggregate, or process data must include the disclosure of which data might be sold or shared, what parties might gain access to the data, to which countries the data might be transmitted or hosted, what the data might be used for, and what rights workers have over their own data.

**The administration should prohibit some forms of illegitimate surveillance that blurs barriers between on- and off-work:** Workers should have a reasonable expectation of privacy off-work hours and in their homes. Employers should not be able to surveil their workers off the job or at home, including location tracking software on handhelds or required on workers personal phones, social media monitoring, or controlling webcams of teleworkers homes, or other intrusive, non-work-related monitoring.

**The administration should move to protect workers from unfair algorithmic treatment and provide remedies and human review:** Employers use surveillance-driven productivity and worker evaluation tools to discipline and even fire workers — in some cases workers are terminated by app. A 2018 study found that most workers had negative emotions about algorithmic decisions around hiring and performance evaluation because the determinations lacked the human traits of understanding context and qualities as well as intuition. Workers have little recourse from these disciplinary activities that can harm their earnings (lost pay, worse shifts, demotions) or cost them their jobs. Workers must have the right to review the data used to make these determinations, know how the data was evaluated that contributed to the disciplinary decision, and correct any errors in the data and the determination. Workers should have the right to remedy errors and demand that a human manager review any disciplinary decision.

**Workers must be critical stakeholders in any artificial intelligence accountability or trustworthiness assessments:** Workers are increasingly subject to artificial intelligence tools in the workplace and must be stakeholders in any assessments of these technologies. No artificial intelligence audit or impact assessment can be meaningful if it excludes the subjects of the artificial intelligence tools. The workers who are subject to algorithmic management and automated surveillance are the people that face the negative repercussions — from firings and disciplinary actions, workplace injuries, heightened stress levels, to illegal discrimination or violations of labor laws. These assessments must engage workers during the design, development, and deployment phase but also these assessments must continue with regular, periodic assessments after the artificial intelligence is deployed in the workplace when it has learned, evolved and changed with changing impacts on workers.

---

319 Lee 2018 at 9 and 11.
The administration must make sure that federal procurement of automated surveillance, algorithmic management, and other artificial intelligence products do not harm workers or reduce service quality: The federal government should not be purchasing automated surveillance, algorithmic management, and other artificial intelligence products that can harm workers without receiving workers’ input and consent before deployment, disclosing all worker-affecting technologies to workers, implementing data-minimization directives, prohibiting the sale or commodification of worker data, prohibiting worker surveillance outside of work hours or on personal devices, providing human review of all worker career-affecting decisions, and giving workers a meaningful voice in all technology assessments and review that affect workers.

The administration must address a host of algorithmic harms faced by gig workers: Platform companies use algorithms to assign tasks, control workers specific task performance such as routes, determine pay per task, rate and evaluate workers based on opaque metrics that workers have charged have been discriminatory, and discipline or deactivate workers without workers right to challenge the algorithm — all of which undermine workers’ pay and economic security.

The administration should not undermine domestic efforts to regulate automated worker surveillance or algorithmic management in digital trade agreements: The existing language in digital trade agreements grants broad authority to tech companies and employers over data and software and severely constrains government oversight of data and algorithms. The administration must not undermine domestic efforts to curb the negative impacts of algorithmic management, automated worker surveillance, and artificial intelligence on workers by pursuing trade deals that severely limit the rights of governments to protect workers, their data privacy, enforce current labor and employment and civil rights law against automated systems, and address emerging threats to workers, people, and society posed by a rapidly changing digital economy.

Thank you for the consideration of our views.

Sincerely,

Amanda Ballatyne
Director
AFL-CIO Technology Institute
My name is Yesenia Barrera. I was a seasonal Amazon warehouse employee in 2019 at the Rialto, California fulfillment center. I am currently an organizer with the Warehouse Workers Resource Center. My Amazon job was the most physically and mentally exhausting job I have ever had. I walked in on my first day excited to be working there, but the joy quickly faded, because of the model of working until you are hurt, driven by the use of technology to constantly track worker productivity.

Amazon warehouse workers carry, bend, reach, twist, unwrap, rewrap and pack items that weigh between 30 to 60 pounds, day in and day out, walking 10 to 15 miles daily with no chance to properly rest our bodies. The work is fast. I tried to hit 200 items an hour and extremely brutal on the body, for shifts as long as 12 hours, although I usually worked ten hours a day.

The surveillance system constantly monitors worker productivity—how many items we pack per second and per hour. If you have not scanned or moved a box for a couple of minutes, the system alerts a manager. It is really stressful and physically demanding to keep up. They never told us if we were making rate, so you are never really sure how well you are doing. Managers just told us to keep going. The pressure forces workers to work faster and faster at the cost of our bodies. Failing to keep the pace can result in a write-up or worse. I was constantly stressed out by having to work fast and even ignored my personal needs for restroom breaks or water because I feared being written up and terminated.

Even though I felt the stress of being tracked all the time, I only learned how pervasive the camera and scanner monitoring system is. One day, I fell behind and boxes started piling up on the conveyor belt. I set down my scan gun to move some boxes aside, and my scanner got buried in the pile. In the panic to pull my scanner free so I did not lose time, I pulled so hard to dislodge it that it bounced back and hit me in the eye. I saw black. Then my supervisor showed up. I thought to myself, how did she know I was not scanning? She had not been in the area. At Amcare, they gave me a wet paper towel and an ibuprofen, and after about five minutes, both my manager and the clinic medic told me I was fine enough to return to work.
It became clear to me then that Amazon tracks your every move the moment you clock in and that unrealistic quotas are why workers are getting injured. After that, I was approached by my manager because the monitoring system said I was not productive enough that day. He told me I was getting a write up and asked me why I had so much TOT. He wanted to know how many times I had used the restroom. I went to the bathroom three times during my entire shift, but it took five minutes to walk each way across the warehouse floor to get to the bathroom, so that time adds up. When I returned for my next scheduled shift two days later, as it did for other workers like me, even though we were working as hard as we could.

That is why I was part of a coalition who advocated for the passage of California Assembly Bill 701, which has brought this punishing, algorithm-driven work out of the shadows by requiring employers like Amazon to disclose workplace quotas and stop penalizing workers for time off task when we comply with health and safety standards. Several other states like New York and Minnesota have followed suit because warehouse workers across the country continue to have the same experiences that I did.

The pace inside Amazon warehouses is unsustainable. I rarely saw anyone leave their station to use the restroom unless they asked someone to cover them. We would ask each other, ‘Do you mind scanning an item every three minutes just so my TOT does not accumulate?’ My coworkers would complain that they would get time off task when they were on their period. Even now, Amazon workers in the Inland Empire say they are harassed for taking too much time in the bathroom, and feel like the easiest way to deal with it is to tell male managers ahead of time when they are on their period.

Amazon treats its workers like robots. We are human. Many of my coworkers lost their jobs because they could not make rate or because of time off task, fueling the high turnover rate at Amazon. Workers who were not fired might work faster, at the cost of their bodies. Workers are getting injured to meet this pace of work for Amazon same or two day delivery. The surveillance system and unsafe pace of work at Amazon should be addressed nationally so that no more workers get hurt. The White House should also look into this surveillance system and its implications for the right of workers to organize. Our federal government needs to make sure Amazon is not a model for other employers and our expectations of workplaces in the 21st century.
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0178
Comment on FR Doc # 2023 12995

Submitter Information

Email: [redacted]
Organization: Center for Democracy & Technology, et al

General Comment

Please see the attached document for our comments in response to this Request for Information.

Respectfully submitted by:

Center for Democracy & Technology
Governing for Impact
Accountable Tech
American Civil Liberties Union
Communication Workers of America
Jobs With Justice
Leadership Conference for Civil and Human Rights
National Employment Law Project
National Women’s Law Center
Open MIC
Service Employees International Union
TechEquity Collaborative
United Auto Workers
Upturn

Attachments

CDT et al - Workplace Surveillance Comments to OSTP
June 29, 2023

To: White House, Office of Science and Technology Policy
   Executive Office of the President
   Attn: Alan Mislove, Assistant Director for Data and Democracy
   Eisenhower Executive Office Building
   1650 Pennsylvania Avenue
   Washington, D.C. 20504

Re: Comments on Automated Worker Surveillance and Management

The undersigned organizations respectfully submit these comments in response to the White House Office of Science and Technology Policy (OSTP) Request for Information on Automated Worker Surveillance and Management, dated May 2, 2023. We thank the White House and the OSTP for highlighting and seeking comment on this vital and increasingly prevalent issue.

Our comments address the risks that arise when electronic surveillance is combined with automated management (together, ESAM) to monitor and control workers. Our comments are organized around the different types of threats that ESAM poses to workers, specifically:

- How these tools threaten the health and safety of workers;
- How these tools are used in ways that discriminate against vulnerable workers and exacerbate structural inequalities in the workplace and labor market;
- How these tools can chill and infringe on workers’ rights to organize and to engage in protected labor activities; and
- How companies use these tools to deprive workers of earned compensation.

These comments both describe the threats that ESAM poses in each of these areas and propose policy steps that federal agencies can take to prevent or mitigate those harms.

I. Definitions and Background

A. Defining electronic surveillance and algorithmic management (“ESAM”)

We use the definition of ESAM endorsed by National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo in an October 2022 memorandum: “a diverse set of technological tools and techniques to remotely manage workforces, relying on data collection and surveillance of workers to

---

1 Much of Parts I and II of these comments is borrowed from a series of memoranda that many of the undersigned organizations, led by Governing for Impact and the Center for Democracy & Technology, sent to the Occupational Safety and Health Administration (OSHA) and National Institute for Occupational Safety and Health (NIOSH) in April 2023. The memoranda focus on the steps OSHA and NIOSH can and should take to address the harmful health and safety consequences of ESAM. See https://governingforimpact.org/wp-content/uploads/2023/04/Surveillance Package.pdf.
enable automated or semi-automated decision-making,” with “remotely manage” meaning that these tools allow employers to manage workers without the physical presence of a human supervisor. There are several categories of workplace surveillance technologies, including remote monitoring, location tracking, keystroke and mouse-click loggers, sophisticated camera and sensor technologies, and scientifically dubious systems that purport to measure emotional states and vocal characteristics. Modern ESAM allows companies to enforce pace-of-work policies that may be intentionally obscured from workers to create an atmosphere of urgency. Some employers also use gamification, which describes technology that is meant to solicit employees to work harder or longer “using video game elements, such as digital points, badges, and friendly competition.” Algorithmic management is the overarching system that takes input from surveillance technologies and other data sources and makes assessments – sometimes leading to disciplinary action – and adjustments to increase worker productivity.

The types of technologies that enable ESAM include: handheld devices, point-of-sale systems, mobile phones, fingerprint scanners, fitness and wellness apps, cameras, microphones, body sensors, keycards, electronic communication monitoring, geolocation tracking, collaboration tools, and customer review solicitation. While surveillance of worker activity has a deep and long history in the United States, the advent of new technologies makes it easier for employers to keep close tabs on their workers without expending much time or effort.

ESAM practices are increasingly prevalent in white-collar jobs, particularly as a result of the pandemic-induced work-from-home revolution. But, as a recent Data & Society report explained:

Low-wage and hourly work—including in restaurant, retail, logistics, warehousing, agriculture, hospitality, domestic work, and healthcare—is more susceptible to datafication because these jobs’ tasks are easily measured. These workers are also often immigrants, women, and people of color, populations historically facing higher scrutiny and levels of surveillance and monitoring.

---


The datafication of work has opened up numerous new avenues for employers to surveil and remotely manage workers.9

B. ESAM is pervasive throughout the economy and is increasingly used in ways that threaten workers’ health, safety, dignity, and legal rights

Large companies frequently use ESAM technology to monitor their workers, and the practice is increasingly prevalent throughout the economy. The pervasiveness of ESAM is a result of cheaper and omnipresent technology, declining levels of worker power, and weak workplace regulation.10 While there are no scientific studies indicating how many companies are using these technologies — and companies are generally not required to report or disclose their use — a 2018 survey of 239 large corporations found that more than half were using “nontraditional monitoring techniques,” and projected that the number would grow to nearly 80 percent by the end of 2020.11

The meatpacking and agricultural industries are both sectors in which ESAM is heavily employed to enforce intense line speeds and production quotas. Quotas and line speeds have long been tools of control for meatpacking management to keep an eye on production, but some of the largest companies are now investing in ESAM technologies like wristbands that track the movement of workers’ arms as they make their cuts.12 In the agricultural sector, guest workers, for example, face punishing quotas.13 The penalty for failing to meet such quotas can be severe, including job loss and subsequent deportation.14

Amazon, the second largest private employer in the United States,15 has heavily used ESAM to monitor its workers and ensure they meet demanding production quotas. In the company’s warehouses, for example, workers are monitored by artificial intelligence-enabled surveillance cameras, which track their movements, and by item scanners, which measure the amount of time that passes between scans and discipline workers for time off task (“ToT”) and for failing to meet their rate goal.16 Outside of the warehouse, the company contracts out most of its delivery business to third parties.17 Amazon uses

---

9 See generally Ifeoma Ajunwa, The Quantified Worker: Law and Technology in the Modern Workplace (2023).
10 Id. at 6.
14 Id.
17 Josh Eidelson and Matt Day, Drivers don’t work for Amazon but company has lots of rules for them, The Detroit News, May 5, 2021, https://www.detroitnews.com/story/business/2021/05/05/drivers-dont-work-amazon-but-company-has-lots-rules-them/4955413001/. As discussed further below in Part III.C, the control Amazon asserts over these workers via ESAM severely undercuts the argument that these workers should be classified as independent contractors rather than employees.
extensive driver surveillance to maintain uniform operations. Amazon imposes a variety of requirements on these drivers, and enforces them through handheld devices that track package drop-offs and determine routes, as well as through artificial intelligence-enabled camera systems that monitor driving behavior. Contract drivers have reported being fired via system-generated email.

Of course, Amazon is not the only firm to engage in this kind of surveillance and automated management of workers. Walmart’s Spark Driver program directs and monitors contract drivers through its mobile phone app, which plans a driver’s routes, the order in which they traverse a store’s aisles, and which parking spot a driver should use. Rideshare companies like Via and Uber tightly control their drivers through ride and job assignments as well as speed-monitoring apps, customer reviews, and cameras.

Outside of the independent contractor context, as early as the 1990s, franchisors were using point-of-sale (“POS”) software to maintain tight control over the employees of their franchisees. 7-Eleven disclaims an employment relationship with these workers, taking the position that the workers are employees solely of the local franchisee and not of 7-Eleven itself, but exerts control over these workers by monitoring the amount of time spent at the cash register and the speed of the ordering process in order to discipline them. By the 2010s, surveillance technology enabled Domino’s and McDonald’s to control their workforce in similar, but more sophisticated, ways. In addition to disciplining workers for slow order processing, Domino’s and McDonald’s required their franchisees to use software that allowed the corporations to dictate worker schedules and screen applicants from headquarters. In a lawsuit against McDonald’s, the NLRB General Counsel detailed the company’s use of technology to compare franchisees’ labor costs to their sales and discipline franchisees accordingly.
Despite the many known examples of intrusive ESAM, however, the full extent to which companies are engaging in such practices remains unknown and, at present, perhaps unknowable. That is because, outside of a handful of states, companies are not currently legally required to disclose the nature or, in most cases, even the existence of workplace surveillance and monitoring. Consequently, the true breadth and depth of ESAM—and, by extension, the risks posed to workers—remains unknown to both workers and policymakers. In this regard, ESAM is a threat to workers that remains uniquely outside of their control and whose true effects may be largely hidden from regulators.

II. Risks to workers’ health and safety & proposed policy interventions

Existing research and documented worker experiences indicate that ESAM has a variety of negative physical and mental health effects on workers. Across a wide range of workplaces, ESAM puts workers’ physical safety and health at risk by increasing the pace of work to unsustainable levels, which results in musculoskeletal strain and an increased likelihood of accidents. Additionally, such technologies contribute to heightened levels of job strain, which has both mental and physical health manifestations. Due to the lack of transparency surrounding ESAM, however, there remains much to be learned about the prevalence of ESAM practices and the effects that they have on workers’ safety and health.

A. ESAM threatens workers’ physical health and safety

Workplaces with higher levels of ESAM deployment often experience an increase in the number of physical workplace injuries. Risk of physical injury arises from the increased pace of work, a decrease in breaks and other forms of downtime that protect workers’ bodies from physical strain, and the physical manifestations of the mental health effects of ESAM.

First, ESAM increases the pace of work, which can be unsustainable and increase the risk of physical injury. Even though some forms of ESAM are marketed as facilitating worker safety by more closely scrutinizing workers’ movements, ESAM tools that speed up processing demands increase the likelihood of injury. For example, Amazon uses ESAM practices to accelerate workers’ pace. Recent surges in demand as a result of COVID-19 led to a series of investigations into Amazon’s employment practices, which include variable quotas, monitoring employees through handheld devices and cameras, and limited breaks. In part as a result of these practices, the rate of serious injuries in some of Amazon’s warehouses is over five times the average for similar workplaces. Monitoring of Amazon-branded delivery contractors has allegedly contributed to traffic accidents and deaths.

28 The California Consumer Privacy Act (CCPA) began applying to employee data in 2023, meaning that California businesses are now required to disclose any collection of “personal information” from their employees. See Cal. Civ. Code § 1798.100 et seq; see also 19 DE Code § 705 (2022) (“Notice of monitoring of telephone transmissions, electronic mail and Internet usage”); CT Gen Stat § 31-48d (2020) (“Employers engaged in electronic monitoring required to give prior notice to employees. Exceptions. Civil penalty”).


20 Id.

21 Reveal, Find out what injuries are like at the Amazon warehouse that handled your packages, (Nov. 25, 2019), https://revealnews.org/article/find-out-what-injuries-are-like-at-the-amazon-warehouse-that-handled-your-packages/.


535
Indeed, Amazon’s record on workplace injuries is such that the company routinely ends up on the Council for Occupational Safety and Health’s annual “Dirty Dozen” list of the least safe American workplaces.33 The Washington State Department of Labor and Industries has cited and fined Amazon repeatedly for forcing its warehouse workers to work at punishing speeds that exacerbate the risk of injury.34 In one such instance, the department concluded that “[t]here is a direct connection between Amazon’s employee monitoring and discipline systems and workplace MSDs (musculoskeletal disorders).”35

Employers across other industries have likewise used ESAM technologies to speed up production with dangerous consequences for workers.36 The meat industry, as noted above, has been able to dramatically increase line speeds in processing and packaging facilities, in part thanks to new surveillance methods.37 These high speeds are part of the reason that the poultry processing industry has some of the highest injury rates in the United States economy.38

Restrictions on breaks and pace of work requirements also pose a significant threat to pregnant and breastfeeding workers who often need to take more time to rest, drink water, use the restroom, and express breastmilk. Such practices have the potential not only to discriminate against pregnant and lactating workers but also to contribute to adverse health and birth outcomes, including miscarriage.39

B. ESAM poses risks to workers’ mental health

ESAM reduces worker control and increases physical and mental demands by requiring them to be busy at every moment, which extensive research has linked to job strain.40 An influential 1979 paper by Robert Karasek first defined job strain as the combination of high “psychosocial workload demands” and low “decision latitude”—a framework often referred to as the “demand/control” model of job strain. Extensive research has demonstrated that job strain is related to anxiety, depression, insomnia,

37 Id.
40 Bossware Report at 4; Constant Boss Report at 12 (“A multitude of data sources drive automated decision-making systems, and such systems are designed to take choices out of workers’ hands”).
and other negative health outcomes. The National Institute for Occupational Safety and Health (NIOSH) has stated that prolonged periods of job strain increase the “rate of wear and tear on biological systems.” This type of stress causes fatigue, and research has linked it to mood and sleep disturbances, upset stomachs and headaches, and chronic health problems like cardiovascular disease and musculoskeletal disorders. In fact, health care expenditures are nearly 50 percent higher for workers who report higher levels of stress.

A large body of research has shown that job strain is strongly linked to depression and anxiety. One 2018 study demonstrated that job strain was strongly associated with serious suicidal thoughts in workers. Studies have also found that fatigue and stress are major risk factors to workplace accidents that can result in physical harm to both workers affected by stress and fatigue and to the workers around them, and that this risk increases the longer workers go without a break.

The implications of this research are alarming given the expanding use of ESAM technologies. Many surveillance practices produce the exact risk factors for job strain: reducing worker control and increasing physical and mental demands by ensuring that workers are busy at every moment. These technologies allow employers to maximize productivity and eliminate even brief periods of worker downtime by continuously monitoring and enforcing a faster work pace. An investigation into Amazon’s surveillance practices concluded that the company’s monitoring of Time off Task through handheld scanners “create[d] the psychological effect of a constant ‘low-grade panic’ ” in the workplace. The fact that employees did not know what productivity rate they needed to hit until they received a warning caused anxiety that followed workers home. These practices worsen the job strain generated by other forms of ESAM, such as the use of scheduling algorithms that often produce erratic and precarious schedules that prevent workers from planning other aspects of their lives.

As NIOSH has noted, job conditions – rather than characteristics of individual workers – are the main drivers of workplace stress. State workers’ compensation systems also recognize the impact of working conditions on mental health. Workers surveyed by Human Impact Partners reported that

---

43 Id.
44 Id.
47 See Constant Boss Report at 12 (“A multitude of data sources drive automated decision-making systems, and such systems are designed to take choices out of workers’ hands”).
49 Id.
50 Id. at 18.
52 See id.
“constant surveillance results in stress, anxiety, and depression.” In 1987, the now-defunct United States Office of Technology Assessment issued a report that highlighted how “monitoring contributes to employee stress by creating a feeling of being watched.”

ESAM may also increase the risk of both mental and physical health impairments because of the opaque and seemingly arbitrary nature of ESAM-driven disciplinary decisions. These characteristics of ESAM may impact organizational justice, a model of job stress that examines “the role of fairness perceptions, e.g., regarding the distribution of resources, the fairness of decision-making processes, and the fairness in interpersonal interactions.” Research indicates that poor organizational justice may increase both feelings of anxiety and depression and the risk of musculoskeletal disorders.

Just as ESAM increases the risk of job strain under the demand/control model, it also increases the risk of job strain under the organizational justice model. When a worker is electronically monitored and is later disciplined or fired through an opaque ESAM-driven system, that reduces organizational justice and increases the risk of job strain—with all the well-documented mental and physical health consequences that follow.

C. Proposed policy interventions

The federal government could take a number of steps to address the health and safety risks that ESAM poses to workers. Earlier this year, a coalition of organizations led by Governing for Impact and the Center for Democracy & Technology sent a set of memoranda to the Occupational Safety and Health Administration (OSHA) and National Institute for Occupational Safety and Health (NIOSH) that includes greater detail on the policy interventions suggested below.

i. NIOSH: Funding research into the health and safety effects of ESAM

By all accounts, ESAM technology is rapidly spreading through workplaces around the country, making research into its effects on workers’ safety and health a top priority. As regulators and legislators begin to take action, they must be able to do so based on scientific knowledge and understanding. Consequently, NIOSH should use its existing statutory authority to fund studies that examine: 1) the effects of ESAM on workers’ mental health; 2) the effects of ESAM on workers’ physical health; and 3) the effects of ESAM on accident rates. These studies should also address the effects of ESAM on workers who are disabled, pregnant, or otherwise protected by law.

---

NIOSH has funded extensive research on both work-related musculoskeletal disorders and on the physical and mental health effects of job strain. For example, NIOSH-funded research found that job strain and long work hours contribute to significantly higher rates of moderate to severe suicidal ideation in working adults.\(^{58}\) Other research indicates that job strain increases the risk of musculoskeletal pain by up to 62%,\(^{59}\) and that job strain significantly increases the risk of requiring a disability pension due to musculoskeletal disorders.\(^{60}\) This potential link between job strain and musculoskeletal disease underscores the need for additional research into the health effects of ESAM. To date, however, we are aware of only one study that examined the impact of electronic surveillance—and that study was limited to computer workers and conducted nearly three decades ago.\(^{61}\)

NIOSH should conduct or commission research in several areas related to ESAM, answering some or all of the following research questions:

- **ESAM and job strain**
  - What are the conditions under which ESAM heightens workers’ risk for job strain?
  - What types of ESAM practices and technology contribute to more severe job strain?
  - What are the rates of job strain and other mental health issues among workers who are exposed to ESAM?
  - What physical diseases, disorders, and manifestations arise in workers affected by ESAM-associated job strain?

- **ESAM and repetitive stress injuries**
  - What are the conditions under which ESAM heightens workers’ risk for repetitive stress injuries and other musculoskeletal injury?
  - What features of ESAM technologies are the biggest contributors to this risk?
  - Does the risk of repetitive motion injuries suggest a clear limit on the “safe” pace of work for workers in particular industries or workplaces?
  - What are the conditions under which mental health and job strain effects of ESAM contribute to physical injury risk?

- **ESAM and industrial accidents**


Under what conditions, if any, does increased pace-of-work lead to more frequent workplace accidents?

Does the risk of workplace accidents suggest a clear limit on the “safe” pace of work for workers in particular industries or workplaces?

- Physical health and safety generally
  - How does employer use of ESAM affect access to reasonable accommodations in the workplace for workers who require and are entitled to such accommodation, including disabled, pregnant, and lactating workers?
  - Do employers’ and vendors’ claims that ESAM technologies reduce injury rates stand up to independent evaluation?
  - Does employer use of ESAM discourage workers from reporting workplace safety and health concerns?

NIOSH should fund both studies that examine how ESAM is impacting workers today, and also longitudinal studies that examine the cumulative effects of ESAM-driven practices over time.

**ii. OSHA should issue regulations and guidance on potentially harmful uses of ESAM**

OSHA should issue rules regulating the use of ESAM in the workplace, including but not limited to ending uses of ESAM that increase the risk of musculoskeletal disorders, job strain and associated health effects, and workplace accidents. OSHA has the legal authority to conduct ESAM rulemaking that covers each of these topics.

OSHA should also incorporate discussion of ESAM into its sector-by-sector guidance on workplace injury prevention and issue new guidance that comprehensively identifies workplace injury risks and solutions in warehousing. OSHA has issued ergonomics guidance to advise employers in some sectors of best practices to prevent musculoskeletal disorders. However, none of these guidance documents discuss the role that ESAM can play in creating ergonomic risk. Additionally, there is not currently a comprehensive ergonomic guidance document for the warehousing sector, in which ESAM and musculoskeletal disorders are both especially pervasive. OSHA should update existing guidance documents for poultry processing and grocery warehousing to include a discussion of ESAM and issue a new guidance document on ESAM risks and solutions in warehousing.

**iii. The EEOC and OFCCP should update existing regulations to address the impact of ESAM on disabled, pregnant, and lactating workers**

As discussed above, intrusive uses of ESAM pose a particularly acute risk to the health of disabled and pregnant workers. Consequently, and as discussed further in Part III, the EEOC and OFCCP should issue regulations under the Americans with Disabilities Act (ADA) and Rehabilitation Act as well as the

---

Pregnancy Discrimination Act (PDA) and the Pregnant Workers Fairness Act (PWFA) (which becomes effective on June 27, 2023), detailing employers’ obligation to ensure that deployments of ESAM do not threaten disabled and pregnant workers’ rights, including their right to reasonable accommodation, and prohibiting uses of ESAM that further harm or marginalize such workers. Similarly, the DOL should issue regulations clarifying employers’ obligations to ensure that uses of ESAM do not threaten lactating workers’ rights under the Providing Urgent Maternal Protections for Nursing Mothers (PUMP) Act.

III. Discrimination and structural inequalities in the workplace and labor market & proposed policy interventions

The increasing use of ESAM in workplaces threatens to dramatically worsen the barriers that workers from disadvantaged groups already face in the workplace and labor market.

A. ESAM practices threaten to further marginalize historically disadvantaged groups of workers

At a basic level, the sheer scale of data that employers collect through ESAM—often without informed or meaningful consent—gives them access to troves of sensitive personal information, including health data, religious practices, family structure, race, gender, sexuality, and nationality/immigration status. For example, data collection on health can capture fertility, pregnancy or other private health data. It is not an unfounded fear that these tools may become additional opportunities for employers to discriminate in the workplace. ESAM has the potential to exacerbate harmful workplace dynamics for Black workers, women, people with disabilities, and other marginalized groups of workers who have long faced greater scrutiny. But ESAM also increases the risk of discrimination and widens existing gaps in the workplace in less obvious but no less impactful ways.

The use of ESAM is heavier in industries where workers are disproportionately from marginalized groups, including people of color, women, and immigrants. It also tends to be used in industries where workers rarely have union protection, leaving them less able to effectively confront exploitative practices.

Additionally, when ESAM is used to impose standardized expectations of behavior, or to identify and flag “atypical” patterns of behavior, workers from already marginalized or underrepresented groups are likely to suffer. A worker with a physical disability may move in ways that an automated video surveillance system identifies as suspicious. Immigrant workers in call centers monitored through speech-recognition systems may speak with accents that the algorithm may not accurately decipher. A tracking system using facial scanning may not function for workers with darker skin. A diabetic worker

---

63 Zickuhr, Equitable Growth Report.
in a warehouse may need to adjust their activity level or take unscheduled breaks or downtime to manage their blood sugar.

Similarly, ESAM tools also may internalize and repeat existing discriminatory stereotypes about how workers from protected groups “should” act or speak. One particularly troubling category of ESAM consists of so-called “emotion recognition” technologies, which have been built into hiring and employee assessment tools and purportedly “promise[] organizations the ability to better know, manage and monitor employees’ interior states and traits.”\(^66\) Even leaving aside the deep privacy and dignity concerns that such tools raise, there is virtually no evidence that emotion recognition systems are scientifically valid,\(^67\) and research indicates that these systems are both less accurate and more likely to assign negative emotional states when analyzing women and people of color.\(^68\) Such tools thus may represent an automated form of the “tone policing” that occurs with women of color, and Black women in particular, and are likely to have outsized negative effects on women, people of color, LGBTQI+ persons, disabled workers, and other historically underrepresented and marginalized groups.

**B. ESAM poses risks for disabled, pregnant, and lactating workers and threatens their right to accommodation under federal law**

ESAM serves as a lever to further heighten the substantial barriers that disabled and pregnant workers have long faced. Disabled people—regardless of race or gender—are more than twice as likely to be unemployed in the United States as non-disabled people, according to the Bureau of Labor Statistics.\(^69\) Disabled workers who work in low-wage and precarious jobs without other financial support are particularly vulnerable to exploitative and dangerous practices because of the need to keep a job, no matter how unsafe or unjust the working conditions—particularly since the ADA currently allows employers to pay disabled workers subminimum wages in some instances.\(^70\) Disabled people of color who face the lifelong impacts of both ableism and racism are also more likely to face systematic employment and hiring discrimination, and to believe they have less bargaining power to ask and advocate for better working conditions.\(^71\)


\(^{70}\) 29 U.S.C. 214(c).

Women—especially Black, Latina, and Native women, women with disabilities, and immigrant women—and LGBTQIA+ individuals have also long been disproportionately likely to experience poverty and hardship. As a result, many women may feel constrained fighting against discriminatory standards and seeking improved working conditions. Pregnant workers face numerous barriers to equal pay and treatment in the workplace. Despite the fact that Title VII and the recently enacted Pregnant Workers Fairness Act protect pregnant workers from discrimination, fully one-fifth of mothers report having experienced pregnancy discrimination in the workplace, and nearly a quarter of mothers have considered leaving their jobs due to a lack of reasonable accommodations or fear of discrimination during a pregnancy.\(^\text{72}\) Women who are pregnant or are perceived as having the potential to be pregnant are at a significant disadvantage compared to men and also to women who are perceived to be past childbearing age.\(^\text{73}\)

ESAM poses unique risks that threaten to exacerbate the disadvantages that pregnant and disabled workers already face. One of the most common uses of ESAM is to increase the pace of work, discouraging workers from taking breaks or downtime and often penalizing them for doing so. Such practices may discriminate against disabled and pregnant workers, who may be more susceptible to new and aggravated injuries and illnesses in the workplace and are expected to comply with arbitrary, automatically enforced standards that do not consider disability- and pregnancy-related needs that may require opportunities for rest, flexibility, and supportive work environments.\(^\text{74}\) Workers with gastrointestinal and urinary tract disorders, for example, may need to use the restroom more frequently or at unpredictable times.

Likewise, many disabled workers, including those with arthritis, musculoskeletal disorders, chronic pain, ADHD, and heart conditions, as well as some workers who are pregnant or lactating, may need to take rest breaks more often. Eliminating breaks also tends to discriminate against neurodivergent workers and those with anxiety disorders, depression, and other psychiatric and cognitive conditions, particularly if combined with intense pacing requirements.\(^\text{75}\)

Pregnant workers who need accommodations may also need more frequent breaks to use the restroom or to rest, and have suffered penalties for taking such breaks.\(^\text{76}\) The lack of adequate break and rest time can have serious health and safety consequences for such pregnant workers, including an increased risk of miscarriage and adverse birth outcomes.\(^\text{77}\) The PWFA and the PUMP for Nursing


\(^{77}\) See Alfred Ng & Ben Fox Rubin, Amazon Fired These 7 Pregnant Workers. Then Came the Lawsuits, CNET (May 6, 2019), https://www.cnet.com/tech/tech-industry/features/amazon-fired-these-7-pregnant-workers-then-came-the-lawsuits/.

\(^{77}\) See Part II.A, supra.
Mothers Act, which built on the Break Time for Nursing Mothers Act, provide new protections for these workers, but workers may face obstacles accessing these protections in the face of ESAM’s automatically enforced standards—workers might be automatically fired for taking breaks guaranteed for them by law. Moreover, ESAM policies and practices may discourage workers from exercising their rights, given the lack of transparency in ESAM systems and the concerns many workers may have regarding retaliation.

Increasingly, employers are setting productivity expectations based on the pace of non-disabled workers, an approach that tends to disadvantage disabled and some pregnant and breastfeeding workers. This is particularly true if the employer does not provide reasonable accommodation, which the ADA requires for disabled workers and the PWFA for pregnant workers. Under the ADA and PWFA, employers must engage in an interactive process with workers who may require disability accommodation to determine “the precise limitations resulting from the disability and potential reasonable accommodations that could overcome those limitations.” The use of ESAM can short-circuit this interactive process.

For example, deaf and hard-of-hearing workers often require communication accommodations, such as ASL interpreters and text communication, that entail the use of intermediaries (whether human or technological). The use of such intermediaries often means that deaf or hard-of-hearing workers need additional time to complete tasks. ESAM systems are rarely designed with such accommodations in mind and, on the contrary, often instead penalize such workers for requiring extra time because automated systems do not account for the right to these accommodations.

Additional breaks are another widely accepted form of accommodation for workers with a wide range of disabilities, but the lack of transparency surrounding ESAM and the productivity quotas that employers enforce through ESAM mean that workers often do not know what accommodations they might need, or are unable to obtain such accommodations in practice.

As a result, ESAM-enforced productivity management often has the effect, or even the purpose, of screening out workers because of their disabilities or pregnancy. Pregnant and disabled workers may be penalized or terminated for failing to meet arbitrary standards, set without regard to their accommodation rights. Some workers may avoid such jobs altogether knowing that they cannot succeed in these jobs without accommodations. In some contexts, such productivity requirements could also result in discriminatory impacts and harms to other protected workers, such as older

---

78 See Jenny R. Yang, Adapting Our Anti-Discrimination Laws to Protect Workers’ Rights in the Age of Algorithmic Employment Assessments and Evolving Workplace Technology, 35 ABA J. Labor & Emp. L. 207, 234 (2021) (aggressive productivity targets could “operate to disproportionately exclude individuals based on protected characteristics,” such as pregnancy, age, disability status, or religion).
79 29 C.F.R. § 1630.2(o)(3).
80 See id.; 29 C.F.R. § 785.18; U.S. Dep’t of Labor, Office of Disability Employment Policy, Accommodations for Employees with Psychiatric Disabilities, available at https://www.dol.gov/agencies/odep/program-areas/mental-health/maximizing-productivity-accommodations-for-employees-with-psychiatric-disabilities (“Breaks according to individual needs rather than a fixed schedule, more frequent breaks and/or greater flexibility in scheduling breaks, provision of backup coverage during breaks, and telephone breaks during work hours to call professionals and others needed for support.”).
workers, women, or people with religious needs. In some agricultural workplaces, for example, productivity standards are based on guestworkers, who are almost all young men, and have contributed to discrimination against women and older workers.

Employers are also gathering workers’ health-related data through workplace wellness programs to try to incentivize workers to increase their productivity. Like some other ESAM practices, some wellness programs try to influence workers’ health decisions through gamification methods, such as web-based challenges where workers receive rewards for completing certain tasks or reaching milestones. Workers with certain disabilities and some older and pregnant workers may not be able to get the benefit of these programs when they are unable to fulfill the criteria or expectations set by these programs, so they are essentially punished for not being as “healthy” as workers who do successfully participate in these programs.

C. Proposed policy interventions

Many of the applications of ESAM described above violate workers’ rights under federal anti-discrimination laws. Employers that use electronic surveillance systems to purposefully single out workers from protected groups for particular scrutiny would violate Title VII, the ADA, the PDA, or the Age Discrimination in Employment Act, depending on the targeted group. Similarly, ESAM that disproportionately flags members of protected groups as engaging in suspicious or disfavored behavior, or that otherwise tends to generate unfavorable evaluations of or actions towards protected groups of workers, may lead to unlawful disparate-impact discrimination. The EEOC should issue regulations or guidance making it clear that ESAM practices that tend to disadvantage protected groups of workers can violate applicable anti-discrimination laws if they negatively impact the terms and conditions of affected workers’ employment.

The ADA provides particularly robust protections for the millions of disabled workers who it covers. An employer that leverages ESAM to automatically penalize disabled workers for taking breaks would likely violate the ADA unless the employer offers an alternative form of accommodation to those disabled workers who generally require more frequent breaks. Likewise, if an employer adopts a faster pace-of-work standard and enforces it rigidly, even against workers with conditions that the increased pace would aggravate, the employer could run afoul of the ADA’s prohibition against “standards, criteria, or methods of administration . . . that have the effect of discrimination on the basis of

---

81 Id.
85 Disability Discrimination in Surveillance Technologies at 54-55.
disability. The EEOC and DOL should issue regulations acknowledging these realities and clarifying that employers should not use ESAM to establish or enforce standards that inherently disadvantage disabled workers.

Like the ADA, the PWFA requires employers to provide workers affected by pregnancy, childbirth, or related medical conditions with reasonable accommodations. Title VII, the PUMP Act, and the ADEA also offer protections to women, older workers and other protected workers who may be harmed by ESAM. The EEOC and DOL should issue regulations and guidance addressing the potential of ESAM to discriminate against such workers.

In the absence of formal rulemaking, informal agency guidance could provide signposts for courts deciding discrimination cases and assist and encourage employers to proactively account for the needs of disabled and other protected groups of workers when deciding whether and how to use these emerging technologies and techniques. The EEOC has issued such guidance with respect to automated decision-making systems for the ADA and Title VII, but that guidance focused primarily on systems that make decisions or recommendations during hiring and promotion processes. This guidance should be updated or supplemented with material that specifically addresses the ADA risks that ESAM poses, as well as employers’ obligations under Title VII, the PWFA, and the ADEA when deploying ESAM or implementing associated practices.

The five principles within the Blueprint for an AI Bill of Rights (AI BoR) also provide the EEOC with a framework to address ESAM practices that disadvantage protected worker groups. The AI BoR states that AI systems must be safe and effective, not discriminate, protect privacy and security, be transparent, and generally allow for the possibility of human alternatives or fallbacks. Marginalized workers should not serve as guinea pigs, and some systems should be prohibited from use outright. If a system is used, it must be vetted by outside audits to evaluate whether it could have a discriminatory impact.

Finally, the administration must prioritize research to better understand and address the impacts of ESAM on the workplace. Greater information is needed about how ESAM is being used and developed; its impact on the workplace and workers generally; how ESAM-driven practices impact protected groups of workers; and what practices and protections best protect workers’ rights and dignity. Research should also identify ways in which ESAM can protect workers’ rights, such as by using ESAM to detect or prevent workplace discrimination and harassment.

---

88 Id.
IV. Interference with union organizing and workers’ labor rights, and proposed policy interventions

A. How ESAM practices are encroaching on workers’ right to organize

In addition to using ESAM to control workers’ behavior in minute detail, companies are using ESAM to identify and disrupt workers’ efforts to organize themselves and push back against harmful workplace practices. Amazon, for example, has sought to hire analysts and purchase software that would allow it to monitor “labor organizing threats” and analyze data on unions.89

The increasing use of ESAM also undermines workers’ labor rights in more insidious ways. As noted in a report published by the Washington Center for Equitable Growth, “the normalization of workplace surveillance weakens worker power by allowing more avenues for companies to justify their anti-union surveillance while also creating a general atmosphere where workers know they are always being watched.”90 Workers’ increasing use of employer-owned computers and mobile devices has blurred the line between work and home life for many workers, which increases the risk that employers will monitor protected organizing activities even when workers are supposedly off-the-job.91

NLRB General Counsel Abruzzo’s October 2022 memorandum directly addresses the threat that electronic surveillance poses to workers’ rights under the National Labor Relations Act (NLRA).92 In it, she identified a number of applications of ESAM and employer actions surrounding their use that could interfere with workers’ right to organize:

- Using surveillance specifically to monitor protected activities;
- Introducing new monitoring technologies in response to protected activities;
- Disciplining workers “who concertedly protest workplace surveillance or the pace of work set by algorithmic management”;
- Using a hiring or management algorithm that discriminates against workers that engage in protected activity (or based on a prediction that they might do so);
- If workers are unionized, failing to provide information about tracking technologies or failing to bargain over them; and
- Using electronic surveillance and a “breakneck pace of work” that “severely limit[s] or completely prevent[s] employees from engaging in protected conversations about unionization or terms and conditions of employment.”93

90 Zickuhr, Equitable Growth Report.
91 Id.
93 Id.
B. Proposed policy interventions

We endorse General Counsel Abruzzo’s useful multi-pronged test for determining whether an employer’s surveillance and management practices violate the NLRA:

- Determine whether the practices, “viewed as a whole, would tend to interfere with or prevent a reasonable employee from engaging in activity protected by” the NLRA. If not, then, the memo implies, the practices would not violate the NLRA.
- If the practices would tend to interfere with Section 7 rights, then the employer must establish several things before use of the technology is permissible under the NLRA:
  - “That the practices at issue are narrowly tailored to address a legitimate business need—i.e., that its need cannot be met through means less damaging to employee rights”;
  - That the business need “outweighs employees’ Section 7 rights”; and
  - That the employer discloses to employees “the technologies it uses to monitor and manage them, its reasons for doing so, and how it is using the information it obtains.”
  - An employer can only withhold such notice if it “demonstrates that special circumstances require covert use of the technologies.”

This standard is both sensible and straightforward to apply. The NLRB itself should adopt Abruzzo’s analysis and use its authority to provide redress when employers use ESAM to interfere with workers’ organizing rights. This would significantly curtail many of the most harmful applications of ESAM.

Additionally, the NLRB initiated rulemaking in late 2022 on a standard for determining joint-employer status. Joint-employer status occurs when two (or more) businesses both act in the capacity of an employer with respect to a particular worker. When this occurs, both companies must adhere to federal labor laws. The crux of the NLRB’s proposed standard is whether each purported employer possesses the “authority to control” or actually exercises the “power to control,” whether directly or indirectly, the terms and conditions of a worker’s employment. In the final rule or a future revision, the NLRB should make clear that the use of ESAM to monitor and manage workers can be evidence of control and thus of employer status.

---

94 Id.
96 Proposed 103.40(c).
V. Wage theft and proposed policy interventions

Companies are increasingly using ESAM systems in ways that may violate workers’ rights under federal wage and hour laws, both by denying workers their lawfully earned wages and by exercising control over workers that companies classify as “independent contractors.”

A. Employers are using ESAM to dock workers’ pay for taking short breaks or for declining to subject themselves to surveillance

The increase in remote work since the start of the COVID-19 pandemic has led to a proliferation of tools that employers use to monitor the productivity of remote workers. Certain ESAM vendors have offered products that integrate with timekeeping and payroll systems, giving employers the ability to automatically dock workers’ pay for time spent away from the computer. Protected workers who may need more frequent breaks, such as certain workers with disability or women who are pregnant or breastfeeding, could be disproportionately impacted by such ESAM-driven practices. Workers may also incorrectly have time deducted for doing work away from their computer, or work that is not readily legible to these tracking systems.

Sadly, there are already examples of ESAM that could be used to deprive workers of earned compensation. Time Doctor, a suite of desktop software with both activity monitoring and time management features, takes periodic screenshots of workers’ computer screens so that employers can determine if the worker is on-task. Time Doctor lets workers delete those screenshots, but according to the software’s FAQ, the time period during which the deleted screenshots were taken will be deducted from the worker’s work hours. In other words, if used as the FAQ suggests, the worker would not be paid for the period during which a deleted Time Doctor screenshot was taken. Docking workers’ pay for short periods of inactivity violates workers’ rights under the FLSA, which allows workers to take breaks of up to 20 minutes during the workday without losing pay.

Recent Medicaid requirements regarding electronic visit verification (EVV) have resulted in many home health care workers facing not only increased surveillance, but also lost or delayed wages. Most of these care workers are women, and often women of color or immigrants. Further, the EVV systems

---

98 Despite employers’ obvious ability (illustrated here) to track working time to the nanosecond, they also continue to game antiquated FLSA regulations permitting rounding and automatic break deductions to the detriment of workers’ paychecks. See Elizabeth Tippett, How Employers Profit from Digital Wage Theft Under the FLSA, American Business Law Journal 55(2):315-401 (July 2018), https://www.researchgate.net/publication/325201388_How_Employers_Profit_from_Digital_Wage_Theft_Under_the_FLSA.

99 FAQ - Time Management Software, Time Doctor, https://www.timedoctor.com/faq.html (accessed May 15, 2023) (“If your manager is using the ‘screenshots’ feature, you’ll also be able to see all screenshots that were taken while you were working, and can delete any screenshots that you choose (the associated time would also be deducted from your work hours).”).

100 See, e.g., 29 C.F.R. § 785.18 (“Rest periods of short duration, running from 5 minutes to about 20 minutes ... must be counted as hours worked.”). This issue is discussed further in the policy interventions section, below.

require workers to manage a demanding technology—time for which they may not be paid—on top of their challenging jobs.\textsuperscript{102}

**B. Some companies are using ESAM to obfuscate and mislead gig workers regarding their compensation**

Compensation for gig workers is opaque and confusing to begin with; a 2021 report by the Pew Research Center found that fewer than half of gig workers understood how the companies for which they work determine how much they get paid.\textsuperscript{103} Some gig platform companies use ESAM in ways that both increase this information asymmetry and exploit it to reduce gig workers’ pay and lure workers into jobs that pay far less than promised or advertised.\textsuperscript{104} Companies also use algorithms to engage in algorithmic wage discrimination, using data mining and ESAM to estimate and pay the lowest amount the system estimates an individual worker will accept to engage in desired behaviors.\textsuperscript{105} The underlying algorithms are opaque and error-ridden.\textsuperscript{106}

Such practices sever the longstanding relationship between time spent laboring and income earned. In addition to the concerns that algorithmically determined wages will not meet a minimum wage, an unpredictable (to the worker) and opaque wage calculation mechanism deprives the worker of any insight into how the firm values their labor and of any predictability in their ability to earn a sufficient sum. Some gig-economy platforms exploit this ambiguity by combining low overall pay with volume and time-based incentives that maximize workers’ time on the platform while minimizing workers’ take-home pay.\textsuperscript{107}

**C. Employers are increasingly using ESAM to exert control over workers (mis)classified as “independent contractors”**

Some of the companies behind gig economy platforms also pioneered ESAM systems to manage their workers. Many of those same companies attempt to classify their workers as independent contractors rather than employees, in an effort to avoid the legal obligations that arise from the employer-employee relationship. But the use of ESAM can be evidence that such employers actually exert a high level of control over workers and have misclassified them.

Under the FLSA, the employer’s right to control a worker’s on-the-job activities is “strong evidence suggesting the existence of an FLSA employment relationship.”\textsuperscript{108} Installing location trackers, cameras,

\begin{thebibliography}{10}
\bibitem{102} Virginia Eubanks & Alexandra Mateescu, ‘We don’t deserve this’: new app places US caregivers under digital surveillance, The Guardian, July 28, 2021.
\bibitem{106} Id.
\bibitem{108} U.S. Department of Labor, Wage and Hour Division, Independent Contractor Status Under the FLSA: Withdrawal, 86 FR 24303 (May 6, 2021) (citing Razak v. Uber Techs., Inc., 951 F.3d 137, 145 (3d Cir. 2020)).
\end{thebibliography}
and digital monitoring equipment and software that continuously track a worker’s activities and assess performance dramatically increases a company’s right (and practical ability) to control the timing and manner in which the worker completes their tasks. Companies who engage in such practices while continuing to treat their workers as “independent contractors” are trying to have it both ways—exercising the control of employers while avoiding the legal responsibilities and obligations to workers that come with that status. This practice often deprives workers of crucial protections under employment laws, such as minimum wage and family and medical leave, and anti-discrimination laws as well as essential employment-based benefits, like healthcare coverage.

D. Proposed policy interventions

i. The DOL should issue regulations prohibiting automated time-docking for ESAM-detected breaks

The FLSA prohibits employers from requiring employees to clock out or docking their pay if they take brief breaks during the workday, briefly engage in non-work-related activities, or have short periods where they are not at their assigned workstation. The Department of Labor’s (DOL’s) FLSA regulations state: “Rest periods of short duration, running from 5 minutes to about 20 minutes . . . must be counted as hours worked.” While the FLSA does not require employers to allow employees to take rest or bathroom breaks and generally allows employers to discipline employees for taking unpermitted or excessive breaks, the employee must still be paid for any brief breaks taken during the workday, regardless of whether those breaks are required by law or permitted by company policy.

Unfortunately, and as the continued public marketing of features like Time Doctor indicates, the illegality of ESAM-driven practices contrary to these established rules does not appear to have deterred some employers from adopting them. DOL should issue FLSA regulations addressing time docking for periods where an ESAM system perceives a worker as temporarily inactive or because workers decline to subject themselves to surveillance.

ii. DOL and NLRB should issue rules or guidance stating that the use of ESAM is evidence of employer status

DOL is currently reviewing comments in response to a Notice of Proposed Rulemaking (NPRM) published in October 2022 regarding employee or independent contractor status under the FLSA. The

---

110 29 C.F.R. § 785.18 (“Rest periods of short duration, running from 5 minutes to about 20 minutes . . . must be counted as hours worked.”).
111 Id.
112 See, e.g., Sec’y United States DOL v. Am. Future Sys., 873 F.3d 420, 426 (3d Cir. 2017) (employer violated FLSA when it required workers to log off for any breaks during workday, and docked workers’ pay if they logged off for more than 90 seconds); U.S. Dep’t of Labor, Wage & Hour Div., Opinion Letter Fair Labor Standards Act (FLSA), 1996 DOLWH LEXIS 39, 1996 WL 1005233, at *1 (Dec. 2, 1996) (work breaks are paid time even if taken “for a myriad of non-work purposes – a visit to the bathroom, a drink of coffee, a call to check the children, attending to a medical necessity, a cigarette break, etc . . . without regard to the relative merits of an employee’s activities.”).
113 U.S. Department of Labor, Wage and Hour Division, Employee or Independent Contractor Classification Under the Fair Labor Standards Act, 87 FR 62218, Oct. 13, 2022. See also Center for Law and Social Policy & Governing for Impact, Comments Regarding DOL’s Notice of
DOL’s proposed rule explicitly stated that the use of electronic surveillance to monitor workers’ activities constitutes evidence of control, and therefore weighs in favor of employee status. DOL should similarly update its joint-employer standards to clarify that the use of ESAM to control workers weighs in favor of a finding of employer status.

A recent NLRB decision tightened the standard that that body will use to determine employee status under the National Labor Relations Act, returning to a common-law standard that considers factors such as the employer’s exertion of control and whether work is performed without supervision. The NLRB should clarify in future decisions that the use of ESAM is strong evidence of control and supervision, and thus indicates that a worker is an employee rather than an independent contractor.

iii. The FTC should issue rules prohibiting gig platform companies from leveraging ESAM to engage in misleading or opaque pay practices

Last year, the FTC issued a policy statement stating that its unfair or deceptive acts or practices authority could apply to the use of automated systems to limit gig workers’ compensation. The FTC should build on this policy statement with formal rulemaking and enforcement action targeting opaque and arbitrary ESAM-driven pay practices that mislead workers and reduce their pay. Similarly, the FTC should use its enforcement authority to penalize companies whose recruitment, advertising, and marketing materials misrepresent workers’ actual pay as a result of the use of ESAM.

The FTC also recently provided a policy statement on biometric information. The policy statement notes that failure to accurately disclose biometrics being used or to assess reasonably foreseeable harms may constitute an unfair or deceptive practice. Because many ESAM technologies collect and use biometrics, and ESAM-driven practices pose a wide range of potential harms to workers, the FTC should scrutinize employers’ ESAM practices as part of its biometrics enforcement.

---


Id.
VI. The federal government should restrict harmful uses of ESAM within the federal government and by federal contractors

The federal government has the ability to restrict harmful uses of ESAM by ensuring that the millions of citizens employed by federal agencies and contractors are not subjected to ESAM practices that threaten their health, safety, dignity, and legal rights. The Office of Personnel Management (OPM) and Office of Management and Budget (OMB) should conduct a study to determine how the various arms of the federal government and their contractors currently use ESAM to monitor and manage federal workers. Those agencies should then issue rules and guidance to ensure that federal agencies refrain from potentially harmful uses of ESAM, unless such uses are necessary due to transparency laws, national security requirements, or other compelling interests.

In those instances where the use of ESAM is deemed necessary, rules and personnel policies should ensure that federal workers are given adequate notice of the nature and purpose of any surveillance or data collection, as well as information regarding how any information collected by ESAM is used in personnel decisions. Under no circumstances should discipline or termination decisions be made based on ESAM-collected information without adequate human review.

Similarly, DOL’s Office of Federal Contractor Compliance Programs (OFCCP) should prohibit federal contractors from using ESAM in a manner that undermines workers’ health, safety, dignity, or legal rights, and should issue rules ensuring adequate transparency and accountability when contractors do use ESAM. Last fall, OFCCP proposed revisions to its audit scheduling letter that called for employers to provide “[d]ocumentation of policies and practices regarding all employment recruiting, screening, and hiring mechanisms, including the use of artificial intelligence, algorithms, automated systems or other technology-based selection procedures.”119 OFCCP should adopt the revised scheduling letter and update the letter further to require employers to submit information on any ESAM systems and practices that the contractor uses to monitor, manage, or direct workers.

Conclusion

While there are, as yet, no federal laws that directly address the use of ESAM in the workplace, existing federal statutes and regulations provide the Administration with ample authority to address the risks that ESAM poses to U.S. workers. In addition, proposed legislation such as S.262, the Stop Spying Bosses Act, which was introduced in the Senate earlier this year, would bring some much-needed transparency to employers’ use of ESAM and place some important guardrails around ESAM-driven practices. We urge the Administration to consider supporting this important legislation. But the administration need not wait for Congress to protect our workers. It can and should take concrete steps, such as those outlined in these comments, to ensure that technological advances are not used in ways that harm workers, particularly those who are already vulnerable and marginalized.

We thank you for your attention and look forward to engaging with the Administration further on these issues in the future.

Respectfully submitted by:

Center for Democracy & Technology
Governing for Impact
Accountable Tech
American Civil Liberties Union
Communication Workers of America
Jobs With Justice
Leadership Conference for Civil and Human Rights
National Employment Law Project
National Women’s Law Center
Open MIC
Service Employees International Union
TechEquity Collaborative
United Auto Workers
Upturn
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0179
Comment on FR Doc # 2023 12995

Submitter Information

Email: [redacted]
Organization: Flex

General Comment

Please see the attached comments from Flex.

Attachments

6.29.23 Flex_OSTP RFI on Automated Technologies
June 29, 2023

Mr. Alan Mislove  
Assistant Director for Data and Democracy  
Office of Science and Technology Policy  
Washington, DC  20500  

Re: Request for Information: “Automated Worker Surveillance and Management” (88 FR 27932)

Flex respectfully submits these comments in response to the White House Office of Science and Technology Policy’s (“OSTP”) Request for Information (“RFI”) issued on May 1, 2023.

I. Introduction

Flex represents America’s app-based rideshare and delivery platforms and the people who use them. Nearly 23 million people have turned to app-based platforms to create opportunities to live, work, and run their businesses on their own terms. App-based work provides individuals with the means to determine where, when, how often—and with which platforms—they want to earn income. This premise has drawn a diverse array of people to our members’ platforms—including parents, caregivers, veterans, students, and entrepreneurs.

At the same time, the app-based economy supports economic growth in communities across the United States and has become crucial in meeting important community needs by facilitating reliable transportation options, supporting individuals with disabilities or illnesses, and providing access to food and other essentials.

Technological innovation has made flexible, independent work available to more people than ever before and has transformed the way consumers secure goods and services. Workers have unparalleled freedom and control over the time they choose to spend earning on and across platforms—autonomy that is distinct from the close and deliberate management associated with the traditional employer-employee relationship.

Therefore, it is important that OSTP distinguish between the ways in which traditional employers are deploying automated technologies to monitor employees’ working habits, processes, and productivity levels as a tool to manage and control the employment relationship versus how app-based platforms deploy automated technologies to maximize app-based workers’ earnings opportunities, unlock new innovations that improve safety and enhance the experience for all users, and increase choice and transparency for app-based workers.

Further, just as millions leverage app-based platforms to unlock income earning opportunities in ways that make sense for them, millions more count on these platforms to better meet the demands and responsibilities of their lives. App-based platforms have proven to be key tools for providing access to reliable transportation, supporting individuals with disabilities or illnesses, and increasing access to food and other essential goods.
Examples also abound of app-based platforms helping communities tackle food insecurity, aid food banks, provide more equitable healthcare, and recover from natural disasters. In addition, the nature of the app-based economy has yielded important data points that are valuable to public decision makers, particularly at the state and local level. App-based platforms engage in information-sharing partnerships with states and municipalities geared toward enhancing key aspects of community infrastructure.

Technological innovations have facilitated the economic and community benefits outlined above. App-based platforms deploy data-driven automated technologies to facilitate a safe, reliable, and efficient experience for the entire ecosystem of their users—including earners, consumers, and businesses—at scale. These are tools and systems that drive and enhance the safe operation of these platforms while preserving worker autonomy and a marketplace that provides value to its entire user community.

Therefore, we appreciate OSTP’s RFI and attention to this important issue. These technologies contain great potential—some of which is already being realized. We also agree that fostering trust and protecting privacy are key goals in an era where digital technologies are enabling and transforming the economic landscape. To that end, we believe that it is critical that policymakers approach this issue in an even-handed way that reflects deep and thoughtful engagement with all elements and stakeholders.

Flex appreciates the opportunity to submit the following comments to help inform policymakers about the ways in which automated technologies are utilized across app-based platforms to the benefit of consumers, communities, earners, and businesses across the U.S.

II. App-Based Platforms Deploy Automated Technologies as Tools to Benefit Workers and Consumers

OSTP’s RFI focuses in large part on the ways in which traditional employers are using a range of technologies to monitor, manage, and evaluate their workers, often for the purpose of increasing

---

1 See David Downey, California city first in US to partner with DoorDash to deliver food to hungry households, The Mercury News (Nov. 3, 2022). Available at: https://www.mercurynews.com/2022/11/03/riverside-joins-with-doordash-to-deliver-food-to-hungry-households/.


4 See Lyft, Disaster Response (September 30, 2022). Available at: https://www.lyft.com/blog/posts/help-after-hurricane-ian (noting Lyft is providing “access to free and discounted rides to help those affected [by Hurricane Ian] in Florida move to designated shelters and critical resources.’).

5 Discussed in greater detail below.
control over their employees. Flex represents app-based platforms that match consumers with independent contractors who can provide services to the consumer. As such, the individuals who choose to provide services on app-based platforms do so with true autonomy—defined by the ability to determine when, where, how, over what duration, and with which platforms they choose to pursue income and work opportunities. This is distinct from the close and direct supervision that employers exert over the workers with whom they engage under a traditional employment relationship.

App-based platforms leverage automated technologies to process information—a foundational element to any technology platform. These technologies have allowed app-based platforms to create efficient marketplaces at scale while helping enhance the safety of these marketplaces for their entire user communities. As we detail below, app-based platforms are using automated technologies to:

— create and maximize earner opportunity and consumer value;
— advance the safety of earners and consumers;
— provide transparency and support earner and consumer decision making; and
— produce data insights that benefit cities and communities.

A. Automated Technologies Help Create, Scale, and Maximize Worker Opportunity and Consumer Value

Automated technologies have enabled app-based platforms to deliver a new service model to communities across the country and scale their respective business operations, connecting millions of people across their networks at any given moment. Over the past 15 years, this innovation has challenged the status quo and the market structures that have defined the provision of transportation and delivery services. The growth of two- and three-sided online marketplaces via app-based platforms has increased access to mobility and goods for millions of people—and at scales and speeds unimaginable even a generation ago.6

This type of technological advancement has delivered immense benefit. App-based platforms have created earnings opportunities for millions of Americans, including those that have historically been left on the economic sidelines.7 At the same time, platforms have connected

---

6 For example, in 2023, the Uber platform was available in over 70 countries and connected consumers with over 7.6 billion trips. (See Uber, 2023 Environmental, Social, and Governance Report. Available at: https://s23.q4cdn.com/407969754/files/doc_downloads/2023/04/Uber-2023-Environmental-Social-and-Governance-Report.pdf?uclick_id=6f5ec9dd-5105-4dce-b643-6af81e45e7b2). Meanwhile, Shipt’s platform is available in 5,000 cities across over 130 retailers. In 2022, Shipt added nearly 1,000 new merchant partners that will allow an additional 2 million households to access the platform. (See, Shipt, Delivering Results: A Shipt Business Snapshot (2021). Available at: https://corporate.shipt.com/getmedia/019d0783-9ae6-4e1a-9b08-b17ebd7b2f59/FINAL_Shipt-Business-Report-Brief_2021.pdf).

7 App-based platforms provide opportunities for individuals who are precluded from traditional W-2 employment (whether that be attributable to chronic illness, disabilities, caregiving or parental responsibilities, or other realities) to earn income. A recent study estimates that there are approximately 1.52 million people who choose independent contractor work for this reason. See Shapiro, Robert and Stutgen, Luke, The Many Ways Americans Work and the Costs of Treating Independent Contractors as Employees (April 2022). Available at:
consumers with reliable transportation options and access to a broader universe of goods and services. This type of network has proved itself as a boon to the entire fabric of a community—from the small businesses that make up a local economy to the neighborhoods they inhabit.

1. **Automated technologies process complex, hyper-local data sets, which can increase workers’ earning potential while delivering an efficient consumer experience.**

At a basic level, data-driven automated technologies are what make these platforms capable of operating. App-based platforms are powered by the automated technologies that process an underlying data set required to match an app-based worker with the consumer. By processing and considering data points such as traffic, location, geographical factors, and other complex market nuances, automated technologies have made it possible to match earners with a trip or delivery in an efficient and reliable manner. Matching technologies are deployed to streamline the user experience for those working on a platform at any given moment as well as the consumer seeking service. For an app-based worker, these technologies are designed to maximize earning potential by matching an individual with a trip or delivery that they are well-positioned to complete—and to do so safely. In doing so, workers avoid unnecessary wait times, which results in greater earning opportunities as well as an efficient service experience for the customer.

For example, delivery platforms use technology models to estimate the duration of every leg of a given delivery, considering specifics pertaining to merchant partner, time of day, geographic and local realities, and traffic. Automated technologies can process real-time and historical data to estimate the duration of a delivery from start to finish, as well as the duration of every sub-milestone of that delivery (e.g., time it takes a driver to travel to a restaurant, pick up an order, and travel to the customer). This model allows platforms to account for variables including restaurant preparation speed, restaurant location relative to a potential worker, and on the ground traffic patterns. These calculations help match workers with a delivery that represents the most efficient use of their time. In turn, this minimizes the time a worker spends waiting for an order which allows them to spend more time earning. It also provides customers with an accurate estimation of delivery and facilitates quick service provision. At the same time, use of automated traffic data improves worker safety by providing realistic delivery timeframes that reflect real-time road conditions and the other variables that impact delivery duration.

Some delivery platforms use location information as a tool for businesses, workers, and consumers. By leveraging such location information, from restaurant pick-up to customer drop-off, the platforms help drivers ensure they are in the right location and restaurants are able to time preparation more accurately. At the same time, this information may be used to help an app-
based worker quickly and safely communicate with a restaurant to notify the business of their anticipated arrival.\textsuperscript{8}

Rideshare platforms deploy these technologies to consider an array of inputs that aim to decrease time between rides for drivers and reduce wait times for riders. With millions of people—drivers and users alike—accessing a rideshare platform at any given moment, there are countless possible matches between riders and drivers. This reality becomes increasingly complex when considering the external factors—traffic jams, rush hour times, construction, and other congestion patterns—that impact transit daily. Automated technologies allow rideshare platforms to consider the array of real-time, on-the-ground realities at a hyper local level to match riders and drivers as efficiently as possible, at a scale far greater than the historical analog equivalent (if there was such an equivalent).\textsuperscript{9}

The process of matching a driver to a rider has evolved over time. In the early years of app-based platforms, riders and drivers were matched based on the closest available driver. However, two things became clear: 1) while this approach worked well for most, some users experienced longer wait times, and 2) the closest did not always mean the most efficient.\textsuperscript{10,11} In response, rideshare platforms have deployed automated technologies to flexibly assess underlying data such as location, road and infrastructure traits, and traffic patterns to match riders with the most suited driver.\textsuperscript{12} This model has resulted in a user experience that allows drivers to earn more by minimizing the wait time between rides\textsuperscript{13} while maximizing the ability to serve all riders in a given area with a streamlined and reliable service option.\textsuperscript{14}

\begin{thebibliography}{9}
\bibitem{9} For example, a consumer’s ability to access a taxi was historically dependent upon being in a location near taxis in transit and/or knowing the telephone number of a local taxi company. The latter variable was further complicated by the reality that there may not have been a service provider at the time and place needed, requiring the taxi service to dispatch a driver via radio or some other means of communication.
\bibitem{11} For example, the driver physically closest may have faced a route riddled with congestion or a traffic jam. Additionally, matching drivers and riders based on one characteristic alone failed to consider the reality of a local area’s entire demand, which inevitably left some consumers with longer wait times.
\bibitem{13} This model also helps workers select a location or general directional route, \textit{discussed below}.
\bibitem{14} See Uber, Marketplace matching.
\end{thebibliography}
2. App-based platforms deploy automated technologies to serve the needs of communities, expanding access to services and opportunities.

In addition to being foundational to the underlying network element of app-based platforms, automated technologies have made platforms accessible to a broader community of workers and consumers. For example, thousands of Deaf or hard of hearing workers earn on app-based platforms thanks to features built into an app that provide added capabilities for these individuals. Drivers are able to request flashing trip request notifications in addition to the existing audio notification. Riders can be automatically notified when their driver is Deaf or hard of hearing and directed to deliver messages via text should they need to communicate.  

Additionally, one platform has partnered with groups like the National Association of the Deaf to explore app improvements that increase accessibility for this community. Another platform has provided riders with the option to review American Sign Language (ASL) basics in the app should they want to communicate with a driver who uses ASL. These inclusive features are possible at scale thanks to data-informed automated technologies.

B. Automated Technologies Advance the Safety of Earners and Consumers

Automated technologies can help prioritize the safety of the workers and consumers who use app-based platforms, as well as the communities in which they live. These technologies can both help protect communities from bad behavior and facilitate public safety objectives while proactively driving innovative advancements in safety.

1. Automated technologies help protect communities from bad behavior while providing rapid user access to professional support and emergency assistance.

App-based workers have options to implement various tools or supports designed to help protect their safety during their time spent on a platform. For example, rideshare drivers may opt to integrate a dashcam and/or utilize audio recording that captures the entirety of the service provision. Documentation of a safety incident may then be shared via a security report and used to assist with investigations or shared with authorities.

Platforms have additionally adopted technologies that can help detect usage of inappropriate or offensive language in the chat function of an app. If such behavior is detected, the consumer will be warned of potential consequences. Importantly, the worker will be automatically given the option to unassign from the service provision in question.  

Several app-based platforms have also entered into partnerships with ADT, a home security brand, to provide workers with the option of receiving live help from a safety agent. If workers feel concerned or uncomfortable on a trip, they may contact a safety agent in the app and receive


help from a trained professional via phone or silently via text. That safety agent may call 911 for the worker should a situation reach a point of escalation.\(^\text{17}\) Additionally, app-based delivery platforms have partnered with samdesk, a global crisis detection platform, to roll out real-time safety alerts that quickly alert workers, customers, and merchants about an emergency or disaster in an impacted area. In the event of an alert, the platform can suspend operations in the area, including canceling any active services so that workers are able to get—and stay—out of harm’s way. To date, these alerts have been used in response to active shootings, bomb threats, and building fires across the country.\(^\text{18}\)

Automated technologies also provide a means by which workers and consumers can help guard their safety and seek assistance immediately in the case of an emergency. For example, rideshare platforms monitor for instances of unusual activities, such as long stops and route abnormalities. A rider and driver will receive an automatic message should either of these be detected, which will inquire whether help is needed. Riders and drivers can also use an in-app emergency button to call authorities in the event of an emergency, which will allow for sharing of location and trip details. Drivers and riders alike may also allow friends and families to follow their route remotely for an added layer of peace of mind (or just to follow along with their trip).\(^\text{19}\) Data-driven automated technologies let platforms unlock these benefits at scale.

2. **App-based platforms are deploying automated technologies to drive promising innovations in public safety.**

App-based platforms are committed to the safety of the entire traveling public—a community that extends beyond motor vehicle users and into and across the multimodal transportation network. Flex members believe that there is an opportunity to make our roads safer through encouraging safer behavior by all who utilize a platform to get from point A to point B.

As discussed above, automated technologies are core to prioritizing the foundational safety of app-based workers and consumers at scale. At the same time, platforms are at the forefront of deploying exciting innovations that will advance not only the safety of their entire user communities, but the traveling public as well. With more than 40,000 deaths and millions of


\(^{19}\) See Uber, Drive with Confidence.
injuries on U.S. roadways in 2021 alone,\textsuperscript{20} these technologies are poised to have a real impact on our country’s road safety crisis.

Advanced telematics is one example of the technologies that fall under this umbrella. Research indicates that telematics-produced insights help encourage safer driving behaviors.\textsuperscript{21} As such, platforms are beginning to pilot advanced telematics to facilitate greater safety for workers. App-based workers on one delivery service platform are now able to choose to participate in a pilot to better understand and learn from their own driving behaviors to stay safer while driving. Workers participating in the pilot will receive key insights about their driving behavior, including speed, distance traveled, and braking. The objective is not to surveil or control how workers’ driving, but to increase community safety by providing helpful takeaways about their driving. The pilot was launched at the end of 2022 and thousands of workers are participating. The platform will evaluate feedback regarding the pilot to help explore and inform how telematics can be deployed in the future as a tool that meets the needs of app-based workers.\textsuperscript{22}

Another app platform recently launched a program that provides weekly reports to drivers choosing to participate to help inform them of their driving behavior across several areas, including braking, phone positioning, and turning. The program has produced early results that indicate these insights have helped participating drivers in making better informed decisions on the road that advance their safety.\textsuperscript{23}

As communities are increasingly utilizing alternate modes of transport—such as bikes and scooters—app-based platforms are leveraging technology to prioritize safety across the multimodal transit network. For example, some platforms have deployed automated technologies to launch bike lane alerts that remind riders to look for bikes before opening a door when their drop off point is near a bike lane or along a bike route.\textsuperscript{24} Additionally, rideshare drivers have the option to display real-time speed limit alerts that inform an individual via a visual alert when they have exceeded the speed limit.

---


\textsuperscript{22} See DoorDash, Helping Dashers stay safe and focused on the road (February 9, 2023). Available at: \url{https://doordash.news/safety/helping-dashers-stay-safe-and-focused-on-the-road/}.

\textsuperscript{23} In 2022, a 10% decrease in hand-held phone use was observed. See Lyft, Lyft’s Impact on Road Safety (February 7, 2023). Available at: \url{https://www.lyft.com/blog/posts/lyfts-impact-on-road-safety}.

\textsuperscript{24} See Lyft, Lyft’s Commitment to Sharing the Road (April 17, 2019). Available at: \url{https://www.lyft.com/blog/posts/lyfts-commitment-to-sharing-the-road}; See Uber, Uber Signs on as a First Mover of USDOT’s Call to Action for Road Safety (February 3, 2023). Available at: \url{https://www.uber.com/newsroom/uber-partners-with-usdot-on-road-safety}.
3. App-based platforms are partnering with federal, state, and local governments to advance public safety objectives via insights gleaned from data-driven automated systems.

Flex is encouraged that the U.S. Department of Transportation recently endorsed some of the safety innovations discussed above as part of its Call to Action Campaign to eliminate roadway fatalities. Secretary Pete Buttigieg launched the campaign to invite stakeholders to share how they are embracing the National Roadway Safety Strategy’s vision for safer roads. Secretary Buttigieg is correct in saying that we need “to harness better technology” to address the public safety challenge that exists on our country’s roads and streets.25 Several Flex members are proud supporters of the campaign and appreciate the Department’s leadership, as well as its acknowledgement that technology—including some of the examples discussed above—has the potential to play a transformative role in advancing road safety and eliminating fatalities.

Additional examples of Flex members partnering with the public sector to advance safety and infrastructure solutions are provided in Section II.D below.

C. Automated Technologies Facilitate Transparency and Reliability to Support Earner and Consumer Decision Making

Automated technologies are central to an app-based platform’s ability to sustain an efficient and reliable experience for independent workers and consumers. At the same time, by supporting the processing of real-time data, these technologies connect workers and consumers with the tools they need to make choices about platform use and consider where, when, and how to use the network. Indeed, as one study noted, “[w]hile markets in general tend to suffer from information asymmetry, many digital platforms appear to have design features that can enhance market transparency … often in the form of new technologies and incentive systems.”26 App-based workers have unprecedented freedom and control over their working lives, and the automated technologies deployed on platforms provide individuals with the means to maximize that autonomy.

1. App-based platforms deploy automated technologies to create a reliable and consistent marketplace for workers and consumers.

Automated technologies allow a platform to consider a range of factors—including real time supply and demand—to create more opportunities for earners and increase service access for consumers. By processing this information, platforms are able to better maintain a balanced marketplace characterized by steady supply and demand. This type of dynamic model helps the network work for all users by sustaining greater opportunities for workers and increasing access for consumers.

25 See U.S. Department of Transportation, Secretary Pete Buttigieg, National Roadway Safety Strategy Call to Action. Available at: https://www.youtube.com/watch?v=NAXMeLex9LU.

For example, when demand spikes in a given area, price adjustments are designed to attract more drivers\textsuperscript{27} to meet that increased demand quickly and restore the market’s balance to ensure consistent supply and demand. Some riders may pay a premium, and others may choose to wait for demand (and prices) to fall. This approach provides immediate incentives for drivers in the short term but helps maintain equilibrium across a market in the long term. But because rider demand eventually goes down in the midst of a surge, ensuring that the market balance is restored and maintained in the longer term is in the interest of drivers and riders. Platforms aim to strike this complex balance via their respective automated technologies that are able to capture and assess the complex and fluid supply and demand equation, and ultimately produce a more reliable earning experience for drivers and an overall more responsible and positive experience for app users.\textsuperscript{28}

Furthermore, studies have found that the use of these data-driven technologies yield tangible efficiency gains for digital platform workers and consumers. For instance, one study found that “taxi drivers route longer in distance than matched Uber drivers on metered airport routes by an average of 8\%, with non-local passengers on airport routes experiencing even longer routing … [and] [w]e observe significant routing efficiency improvement after taxi drivers became Uber drivers.”\textsuperscript{29} In other words, data-driven automated technologies such as these likely result in significant savings in consumer expenditure and time—fewer missed flights and appointments. And it suggests that these automated technologies have helped app-based earners become more efficient in their routes as they were provided with the information that enabled them to choose more optimal, pro-consumer routes.

2. Automated technologies provide app-based workers with visibility into market conditions.

Many app-based workers continue to choose to earn on Flex members’ platforms because of the ability to choose when and where they work, as well as the ability to determine the duration of their decision to do so.\textsuperscript{30} Automated technologies provide workers with visibility into the current market demand at any given moment—a valuable tool that helps workers form an accurate expectation of what to expect should they choose to log on to the app. For example, rideshare drivers can access information via in-app tools that provide “heat maps” or other means to illustrate where a demand hotspot exists in a given market. These tools also forecast future demand periods in a given area. In this way, automated technologies create a form of network and market transparency that workers can leverage to inform their decisions regarding when, where, and how they choose to utilize an app—and thus help them maximize their earnings.\textsuperscript{31}

\textsuperscript{27} This can include generally funding driver incentives.

\textsuperscript{28} See Uber, What is the right balance? Available at: https://www.uber.com/us/en/marketplace/open-marketplace/marketplace-health/?uclick_id=6f5ec9dd-5105-4dce-b643-6af81e45e7b2.

\textsuperscript{29} Moral Hazard Study.

\textsuperscript{30} According to a 2022 Morning Consult survey, the overwhelming majority of app-based workers (77\%) prefer to remain independent contractors and maintain this flexibility. See Flex and Morning Consult, Worker Survey (September 2022). Available at: https://www.flexassociation.org/workersurvey.

\textsuperscript{31} See Lyft, the Driver’s Guide to Pay. Available at: https://www.lyft.com/driver/pay#earn.
A particularly compelling example of how this technology is used to improve the worker and consumer experience is evidenced at one of the busiest travel hubs in any city: an airport. The nature of an airport makes balancing the supply and demand equation, along with mitigating worker and consumer wait times, increasingly complex. However, a rideshare platform is able to leverage automated technologies to forecast supply balance and optimize driver allocation by considering data points ranging from weather conditions, distribution of arriving flights, and other temporal considerations. Using this model, a platform can produce an estimation of how long a driver would have to wait before receiving a trip request. This gives drivers the information they need to decide whether they would prefer to seek an airport trip or reposition themselves for accepting another ride after completing an airport drop-off. Likewise, providing drivers visibility into periods of low demand may help them decide to stay in a city to optimize their earning time.32

3. **Automated technologies allow workers to choose, control, and direct where and when they earn on app-based platforms.**

Automated technologies also empower app-based workers to deploy precision with respect to where they are interested in working during a given period should they wish to stay within a given radius or pursue a trip or delivery as they travel to another area. Application of technology in this way serves as an efficiency tool for workers to utilize if and when they choose, providing greater opportunities for individuals to flexibly earn on platforms in ways that make sense for the demands of their personal lives. For example, if an app-based delivery worker wishes to use their commute home from another job to pick up a delivery trip, they can select an end location. The platform will then seek to connect the individual with a delivery trip along that route.33 Indeed, survey data suggest this is a frequent use-case for workers.34

These technologies create similar options for rideshare drivers. A driver can use location filters to set preferred arrival times, specify a destination and only receive ride requests in that direction, and set a radius around a given location on a map.35 This is all made possible due to data at scale filtered through automated technologies and systems.


34 For example, DoorDash shares that 52% of workers using the app “choose when they dash around their other responsibilities, like between classes or after work.” Additionally, 60% of workers using the DoorDash app reported that they “combine dashing with a range of their other responsibilities,” including picking up groceries or conducting errands, commuting or traveling, or dropping off or picking up their children. See DoorDash, Delivering the Goods: The Impact of DoorDash in the United States (2022). Available at: [https://downloads.ctfassets.net/trvmqu12jq2l/6zLcMwJ9xOG7CtnYyovCMo/b87905ee2ee48b90abe7b471f4eabbc2/DoorDash-EIR-2022.pdf](https://downloads.ctfassets.net/trvmqu12jq2l/6zLcMwJ9xOG7CtnYyovCMo/b87905ee2ee48b90abe7b471f4eabbc2/DoorDash-EIR-2022.pdf).

D. Automated Technologies Produce Data Insights That Benefit Cities and Communities

Furthermore, app-based platforms are leveraging automated technologies for additional purposes that extend beyond their virtual marketplaces. Automated technologies facilitate data aggregation across a given network that platforms are increasingly utilizing to produce and share insights with leaders at the local level in service of addressing community needs and improving cities. In this way, these technologies generate aggregated information that help to inform important public decisions.

— Preparing the Power Grid for Electric Vehicles (EVs): As EV sales continue to grow and as the Biden administration continues to take steps to build a national network of 500,000 electric vehicle chargers to confront the climate crisis, policymakers at the local, state, and federal levels are faced with important considerations around vehicle charging infrastructure and underlying power grid operation. Utility providers and energy organizations are gathering data that analyze charging trends so that they understand when demand is likely to be highest—information that is needed to prepare in ways that mitigate blackouts or brownouts across their electrical networks. However, they have struggled to find a data set of EV driver behavior that is large enough to derive meaningful results. Flexdrive, an independently managed subsidiary of Lyft that supplies drivers with vehicles to rent through Lyft’s Express Drive program, partnered with Peninsula Clean Energy to help advance this data set. Peninsula Clean Energy subsidizes the cost of 100 rental EVs from Flexdrive available to drivers on the Lyft platform. In exchange, Flexdrive provides the utility with data on when and where the EVs charge, how long each charging session lasts, and what types of chargers the drivers use.37

— Valencia Street Safety Pilot: San Francisco’s Valencia Street is a famous, bustling neighborhood and commercial corridor. It is heavily trafficked by bicyclists, commercial delivery vehicles, passenger vehicles, and pedestrians on foot. As a result, the corridor has experienced growing safety concerns and community organizers have advocated for a redesign. Encouraged by the San Francisco Municipal Transportation Agency’s initial steps to address these concerns, Lyft leveraged their technology to help provide a solution. Through analyzing ride activity throughout the corridor to ascertain high volume pick-up and drop-off locations, Lyft found that limited curb space was a central challenge for the corridor. The company hypothesized that improvements to the Lyft app could help create a better transit experience for riders and drivers while advancing safety. As a result, Lyft established a pilot that designated pick-up and drop-off locations along side streets to address curb space limitations. In evaluating the pilot, Lyft also gleaned additional insights from these datasets.


37 See Lyft, How rideshare data is preparing the power grid for EVs (March 22, 2023). Available at: https://www.lyft.com/rev/posts/how-rideshare-data-is-preparing-the-power-grid-for-evs.
that have been shared with city officials. These range from the need for more loading zones, protected bike lanes that offer physical separation from motor vehicle traffic, a comprehensive curb space management strategy, and clearer wayfinding and signage to direct passengers and riders more efficiently.  

— Cincinnati Mobility Lab: Uber and the City of Cincinnati created the Cincinnati Mobility Lab, a multi-year partnership seeking to develop innovative transportation strategies across the city, local transit, and local business organizations. Like Valencia, curb space in Cincinnati is a resource that multiple transportation modes compete for on a daily basis. Uber commissioned a study that analyzed rideshare pick-up and drop-off activity data, traffic count data, video documentation, and in-person observations to identify potential improvements to curb space allocation and traffic management for city leaders to consider.

III. Looking Ahead and Conclusion

The use of automated technologies across app-based platforms is not new. These technologies are what has allowed platforms to scale their operations safely, efficiently, and in ways that have unlocked tremendous value for independent workers, consumers, and communities. Platforms have gleaned insights from the data points that these technologies capture, along with feedback from the individuals that use their networks to earn income or secure transportation or delivery services. Over time, these combined learnings have prompted platforms to deploy automated technologies in new ways, delivering tools to the entire user community that advance safety, efficiency and opportunity, marketplace transparency, and choice.

As OSTP notes, many of the technologies and systems at the center of the RFI’s focus have developed over recent years and across a variety of contexts. It is important that OSTP distinguish between the ways in which employers are deploying automated technologies to monitor employees’ working habits, processes, and productivity levels as a tool to manage and control the employment relationship versus how automated technologies are utilized in the platform economy.

App-based workers choose to earn on Flex members’ platforms because it provides them the unparalleled ability to secure income on their own terms and with the autonomy to select where, when, how often, and with which platforms they choose to work. Automated technologies have made this type of work accessible at scale while providing a suite of tools that app-based workers may choose to utilize as they seek to optimize their earning experience. While there are differences across platforms, in general, app-based workers enjoy autonomy and control over


their working lives that is distinct from the close and deliberate management that employers exert over their employees, whether that be through the use of technology or otherwise.

Flex acknowledges that there are many emerging applications of automated technologies that carry tremendous potential across the economy and society at large. At the same time, the advent of these innovations, like any other technological advancement, requires all stakeholders across business, academia, the consumer base, and government, to think critically about responsible development, deployment, and oversight. Flex represents companies that are beginning to develop governance frameworks focused on the emerging technological landscape that take into consideration potential use cases and benefits, ethical and risk concerns, and other policies and processes.41

Flex stands ready to work with OSTP and other policymakers as they continue to examine the many technologies at the focus of this RFI. Government must commit to deep, thoughtful, and sustained engagement with all stakeholders as it seeks to understand the varied and evolving use cases of these technologies. Such technologies have the potential to unlock societal benefits that deliver greater economic outcomes, advance safety objectives, improve healthcare and medicine, and achieve climate and sustainability goals, and policymakers must take care to avoid hampering innovation or having a chilling effect on economic development and U.S. competitiveness.

Thank you for the opportunity to submit comments in response to this RFI.

Sincerely,

Kristin Sharp
CEO, Flex Association

---

Public Submission

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0180
Comment on FR Doc # 2023 12995

Submitter Information

Email: [redacted]
Organization: American Foundation for the Blind

General Comment

See attached file(s)

Attachments

AFB Comment on OSTP RFI Automated Surveillance 06-2023
June 29, 2023

Alan Mislove
Assistant Director for Data Democracy
White House Office of Science and Technology Policy
1600 Pennsylvania Ave NW
Washington, DC 20500

Filed electronically via regulations.gov

RE: Request for Information; Automated Worker Surveillance and Management

Dear Assistant Director Mislove:

The American Foundation for the Blind (AFB) is a national nonprofit that advocates for a world of no limits for people who are blind or have low vision by mobilizing leaders, advancing understanding, and championing impactful policies and practices using research and data. AFB has conducted several research studies during the last four years that demonstrate the positive and negative impacts of technological adoption on people who are blind, have low vision, or are deafblind. Therefore, we greatly appreciate that the Office of Science and Technology Policy is soliciting information about how emerging technologies may affect and even discriminate against workers, including workers with disabilities.

Blind people and people with low vision benefit greatly from advances in technology in terms of information access, efficient access to integrated work processes, and communication. However, AFB research has proven that technology used in the workplace often presents significant hurdles that can reverse those potential gains. The barriers may originate in the software or hardware design, but there are also frequent examples of how workplace policy and practice impede the career trajectory of blind and low vision people. Although there is a current deficit of research specifically on automated worker surveillance and monitoring, it is likely that the same barriers that are present in other aspects of workplace technology carry over to surveillance and monitoring tools and their use. Additionally, digital accessibility barriers may impact how automated tools evaluate the productivity, behavior, and
performance of workers who are blind or have low vision. AFB strongly encourages OSTP and other federal agencies to further investigate and respond to the potential discriminatory effects of automated worker surveillance and monitoring tools on workers with disabilities.

What data and evidence exist on how the impact of automated worker surveillance and management systems differs across groups of workers, including based on characteristics such as race, national origin, sex, age, disability, religion, or health status?

In 2022, AFB released the Workplace Technology Study, which explored worker experiences with workplace technologies and accommodation practices. The study found significant disparities in the accessibility of websites, software, and hardware that employees are expected to use during the hiring process, on the job, and as part of their employee benefits. All of these areas are covered by the Americans with Disabilities Act. It is imperative that the Equal Employment Opportunity Commission and other federal agencies investigate, enforce, provide guidance on, and regulate the potential discriminatory impact of workplace technologies, including automated worker surveillance and management systems.

While the Workplace Technology Study produced only limited evidence specifically related to automated worker surveillance, the study did produce a few examples of how workers encountered automated systems in the hiring process and experienced automated employment-related test proctoring. There was evidence that employees face discrimination in the use of eye-tracking software or other tools that surveil an employee or candidate’s body movement. These tools often do not account for differences in body movements that people with disabilities may make and the differences in how and where people who are blind may need to look during their work. One participant wrote:

“[I had to take a] virtual certification exam... I chose to take [the exam] from home thinking this would be less travel and I can use my own equipment. The exam was conducted by a proctor of a third party that observes you via webcam. [To accommodate the testing platform,] I had to take out all my large monitors and take the test via my laptop...I have to really have my face close to the laptop screen and when I have to move my head to look at the remaining time at the right edge of the screen (in small font) the proctor would warn me about keeping my head still. Then after doing this twice, he said next time, he will have to
People with disabilities do not necessarily use so-called “typical” body movements and may interact with their computers and assistive technology in divergent ways. Many blind people may not use their eyes at all, may have prosthetic eyes, or may use dark lenses to protect against light sensitivity, thus nullifying the usefulness of eye-tracking software in determining attention, productivity, and honesty. Other examples of how people who are blind or have low vision interact differently with their computers or workstations includes turning off the screen or navigating offscreen via assistive technology, in which case screen shotting software may not be as effective; using different user interface methods, such as listening to a long document which may not require the user to scroll as frequently; or even switching to a mobile app when the required desktop client is inaccessible.

There was also evidence that automated systems in general are not always accessible, requiring workers and job candidates to request accommodations or find workarounds. It is also important to note that not all job candidates request accommodations out of fear of discrimination, and unpublished analysis of the data suggests that candidates who are both blind and people of color may be even less likely to request accommodations. As described in the report, participants reported “a variety of challenges [with automated pre-employment testing] such as difficulty keeping up with timed assessments, incompatibility with screen readers, small fonts, needing to respond to pictures during the assessment, or needing to take the test on a computer without screen reader software or screen magnification software installed.” If the automated worker surveillance and monitoring systems are not fully accessible to and usable by people with disabilities, they may not be able to check-in to register attendance in a timely manner, impacting hourly pay, or they may not be able to activate a

---

2 Id, 22.
system providing an employer remote control of the employee’s systems. If an employer ties employee pay, promotions, or other benefits to the results of automated monitoring systems, it is imperative that those systems be fully accessible, including with assistive technology.

In addition, the use of automated worker surveillance and monitoring systems does not account for an employee’s challenges with other inaccessible workplace systems and technology. This concern is especially problematic if automated systems are measuring worker productivity and used to discipline, pay, or promote employees without accounting for when the work environment is inaccessible. As noted in the Workplace Technology Study, “The combination of mainstream and [assistive technology] can increase a worker’s productivity, but if the products do not work well together, a worker’s productivity can be decreased. In the same vein, those who do not use AT but have low vision and use built-in features of software may not use the software as efficiently as [a sighted person would], and thus their productivity is decreased.”3 It is not only inaccessible design that produces this effect: Insufficient access to accessible training that takes into account how a blind employee uses assistive technology also is another factor that reduces employee productivity and performance, at least in the short run. In fact, in the Workplace Technology Study, workers who did not receive adequate or accessible training reported “feeling that their productivity was negatively affected and that completing tasks or figuring out training was incredibly time consuming.”4 Employees may be registering as less productive on an automated monitoring system when in fact the employment environment is inaccessible. This can also occur while an employee waits for assistance from an IT professional.

It is also concerning that people with disabilities may also be subject to unnecessary surveillance at home or on personal devices that people without disabilities do not have to worry about. In the Workplace Technology Study, some people who are blind or have low vision reported using personal devices to access software apps required for their work because the desktop client is not fully accessible, or because they did not receive needed accommodations.

3 Id, 34.
4 Id, 59.
210 participants reported that they used the following personal technology tools to complete job tasks for which they did not have adequate accommodations: computers or laptops with screen reader or magnification software (n=121), tablets (e.g., iPad, Android) (n=60), and braille notetakers or refreshable braille displays (n=55). People with disabilities should not be unnecessarily subject to surveillance on their personal devices due to the presence of accessibility issues on their employer-issued hardware, so it is important that controls are limited in the extent to which employers can monitor work-related activities on non-employer owned devices. Conversely, people with disabilities would not be as likely to need to use their own devices if all of their workplace systems were fully accessible and all requested accommodations were provided. This is an example of how closely interrelated privacy and accessibility are for people with disabilities.

On the whole, people who are blind or have low vision do not have confidence that their employer is considering their needs when adopting new technologies. Only 50.2% of Workplace Technology Study participants agreed that their current employer or contractor takes into consideration the accessibility and usability needs of blind and low vision employees and contractors when adopting new software, tools, or apps. We must assume that similar rates of employers are not fully accounting for the needs of their blind and low vision workers when adopting surveillance and monitoring systems.

What data or evidence exists on how the provision of reasonable accommodations is accounted for in the design and operation of automated worker surveillance and management systems?

Although current data is limited, it is reasonable to expect based on other evidence of current employment practices that blind and low vision employees may not receive appropriate reasonable accommodations when automated worker surveillance and management systems are deployed in the workplace. Several areas of potential concern include whether the systems themselves are designed to be accessible to and usable by people with disabilities; whether the

---

5 Id, 39.
6 Id, 55.
systems interfere with or account for the use of assistive technology; whether they incorporate features that allow employers to individualize performance metrics such as time to complete tasks; and whether systems that monitor body language and user inputs account for differences in body type, behavior, and input methods. As one blind employee wrote, "Coming to a new company as somebody who has accessibility needs is usually a nightmare[....] to navigate processes that are optimized for the 99th percentile and they just don’t know how to handle people who have different needs." Any use of automated worker surveillance and monitoring must address the fact that not all workers perform tasks the same way and that reasonable accommodations must be honored in accordance with the Americans with Disabilities Act and Rehabilitation Act.

The accommodations process is dependent on numerous parties within a given company: the employee, the manager, the human resources (HR) manager, and the information technology (IT) manager. It is not uncommon for people who are blind or have low vision to wait significant periods of time (in some cases months) for their accommodation requests to be resolved. In other cases it may take time to optimize requested assistive technology for an individual employee. For example, one participant in the Workplace Technology Study wrote about how the IT systems that their company employed interfered with their use of assistive technology: “With my work computer being a 'managed device,' it was very difficult to obtain approvals to get ZoomText installed as it required ADMIN rights and wasn’t on their list of approved software. Getting IT to assist and bypass approvals was very difficult at the time.”

During the waiting period, the employee may not be as productive or able to access the systems that are being monitored through no fault of their own. Providing accommodations that employees with disabilities require in a timely manner is part of an employer’s obligation under the law, and a failure to do so may constitute discrimination. Additionally, employees may need additional accommodations to manage how they meet performance metrics set by automated monitoring systems during times that their workplace technology is inaccessible.

7 Id, 28.
8 Id, 32.
9 Id, 29.
The role of communication and human oversight of automated monitoring systems is essential to meeting the accommodation needs of people with disabilities.

In general, use of automated worker surveillance and monitoring systems must allow for accommodations for workers with disabilities, especially when other workplace technology is inaccessible, impacting employee productivity metrics, or when the employee needs other accommodations to meet the expected productivity metrics. One participant in our study described that the reasonable accommodation process was not effectively executed and resulted in the participant losing their job rather than receiving meaningful and reasonable accommodations. She wrote, “I was being judged on the same metrics as fully sighted coworkers...which put me at the bottom of the employee ranking, then I was harassed by my supervisor to bring up my numbers...I explained that because of my vision I could not work as fast, I can only see from 1/10 of one eye. My supervisor and HR asked for more medical documents, which I gave, then [they] gave me options which forced me out of my job.”10 It is not unreasonable to expect that when performance measurement is automated, employees with disabilities face discrimination due to inaccessible technology, processes that do not account for employee diversity or their reasonable accommodations, or other stigmatization.

It is also relevant to note that persistent stigmatization of people with disabilities continues to result in job candidates forgoing disability disclosure out of fear of discrimination, meaning that they may not be asking for needed reasonable accommodations. Of 323 participants in the Workplace Technology Study, 53 participants did not disclose their disability. “These participants reported they wanted to get their foot in the door first and previous experience had taught them that if they disclosed their visual impairment early, they would be denied that opportunity.”11 If automated surveillance is used in the recruitment and hiring process, especially during pre-employment testing or interviews, it is imperative that employers follow

10 Id, 62.

11 Id, 21.
best practices for offering and providing accommodations and ensure that the systems do not discriminate against people with disabilities, such as through eye-tracking technology.

Where might further research, including by the Federal Government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?

Because the evidential record is currently limited, the Federal Government has ample opportunity to fund research that explores the impact of automated worker surveillance on people with disabilities and their employment. Factors to investigate include the accessibility of the user interface for employees and managers including those who use assistive technology; whether surveillance systems treat equally people performing work in different ways; whether it is easy to individualize metrics for workers with approved accommodations; whether employers provide ample transparency about the use of these systems that allows employees to request meaningful accommodations; and whether existing federal guidance and enforcement measures are sufficient to prevent and respond to cases of discrimination.

What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers' rights?

Several efforts could help ensure that these systems do not discriminate against people with disabilities. First, employers must understand existing guidance about disability, including the EEOC’s technical assistance document, “The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees.”12 Employers must also implement current requirements for accommodating employees in a timely manner. Although the EEOC has issued guidance on numerous accommodation and discrimination topics, AFB’s research continues to demonstrate that many employers are either unaware of or do not meet their legal obligations toward employees with disabilities.

Second, developers of surveillance and management systems should adhere to existing software accessibility standards, such as the Web Content Accessibility Guidelines, and develop industry standards for testing their products with diverse employee populations, including people with disabilities. Because these systems have the potential to determine employee pay, performance rating, and job security, they must be held to rigorous anti-discrimination standards. These industry standards could be guided by government-funded research that prioritizes the needs of employees and the way people actually work.

Third, employers should adopt best practices that require transparency and accountability in the use of worker surveillance and management systems. People with disabilities already struggle to receive accommodations that work and to receive access to technologies that are fully accessible as soon as they are deployed. However, people with disabilities cannot request accommodations for a process or system that they do not know exists. Therefore, employers should be transparent about which technologies are being used, how and why they are being used, and how they will impact employee advancement, pay, and benefits. At that point, workers with disabilities will be better equipped to request reasonable accommodations.

What policies or actions should Federal agencies consider to protect workers' rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

Federal agencies should reinforce the existing regulatory scheme under the Americans with Disabilities Act and Rehabilitation Act to account for this sector of emerging technologies. First, it is important to issue regulations under Title II and III of the Americans with Disabilities that require websites and software applications to be accessible. The Equal Employment Opportunity Commission (EEOC) should also propose regulations under Title I that cover the websites and software applications used by employers. These regulations should result in the reduction of many of the productivity issues reported in the Workplace Technology Study as well as how many additional accommodations are needed to navigate an inaccessible virtual work environment. In addition, the EEOC or another federal agency should investigate whether
these systems are having disparate impacts on disabled employees’ hiring, pay, advancement, and benefits. With so many of these systems operating in the background and with discrimination existing in other forms, it may not always be easy for individuals with disabilities to understand when an automated system is being used to discriminate against them or to marshal the legal resources to file a complaint in a timely manner. Thus, federal agencies may be better equipped to identify trends and initiate appropriate enforcement actions.

Thank you for the opportunity to provide information about what our research shows about the use of technology and impact of employment discrimination on people who are blind or have low vision, including people who are deafblind. If you have any questions about this issue, please contact Sarah Malaier, (b) (6) .

Sincerely,

Stephanie Enyart

Chief Public Policy and Research Officer
Docket: OSTP-TECH-2023-0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP-TECH-2023-0004-0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0181
Comment on FR Doc # 2023-12995

Submitter Information

Email: [redacted]
Organization: National Employment Law Project

General Comment

See attached file(s) for comment by the National Employment Law Project

Attachments

NELP OSTP Surveillance and Algorithmic Management Comment
June 28, 2023

Comments in Response to Office of Science and Technology Policy ("OSTP"),
Docket OSTP_FRDOC_0001-0004

Submitted via https://www.regulations.gov/document/OSTP_FRDOC_0001-0008

To Whom It May Concern:

The National Employment Law Project (NELP) submits these comments in response to the Request for Information (RFI) on Automated Worker Surveillance and Management initially published by the White House Office of Science and Technology Policy (OSTP) on May 1, 2023.

NELP is a nonprofit research and policy organization with over 50 years of experience advocating for the employment and labor rights of underpaid workers. We seek an equitable, good jobs economy by advancing policies that ensure jobs pay well, provide ample benefits, foster health and safety, and decrease racial income disparities; we also champion robust unemployment insurance for those unable to work. NELP recognizes that corporate respect for worker autonomy, responsiveness to worker voice and judgment, and equitable and transparent decision-making are essential foundations of any good job. Accordingly, we support policies that foster workplace democracy and encourage workers to join together to improve working conditions. NELP works closely with worker centers and other community-based organizations with members who are subject to workplace surveillance and algorithmic management, and we base our comments in part on understandings we have developed through those relationships.

In recent years, corporations have vastly expanded automated or electronic surveillance of workers and reliance on data-driven or algorithmic management. These two practices are distinct, though both pose harms to workers and threaten to degrade working conditions, particularly for workers of color as we explain below. For the purposes of our comments, however, NELP will largely follow the approach of the RFI and refer to both practices together as “Automated Worker Surveillance and Management” (AWSM). Our comments discuss our concern with how corporate adoption of AWSM can exacerbate existing challenges to an equitable, good jobs economy. Specifically, our comments highlight that:

1. AWSM can enable discrimination in recruitment and hiring, and can perpetuate occupational segregation;
2. AWSM enables corporations to mask control and deny accountability, degrading working conditions and fostering racial income and wealth disparities;
3. AWSM can increase barriers to organizing and bargaining collectively, particularly in industries with disproportionately high percentages of Black and immigrant workers;
4. AWSM can combine with other health and safety hazards to amplify unhealthy and unsafe work environments;
5. AWSM is often used to discipline and terminate workers without transparency or meaningful processes to contest decisions, increasing precarity and potentially amplifying race inequities; and
6. AWSM facilitates unfair, unpredictable, and discriminatory pay.

We conclude by highlighting the need to deliberately incorporate worker voice, and we recommend policy reforms.
1. **Data-driven, automated recruitment and hiring systems can be discriminatory and perpetuate occupational segregation.**

Workers’ access to jobs is increasingly mediated by opaque digital hiring systems. In recent years, employers including Amazon, Target, and Hilton, have begun to use data-driven, automated tools to recruit, screen, and select job candidates. These systems often draw on data covering multiple facets of candidates’ personal and professional lives and use artificial intelligence to make predictions about candidate job fit and performance. The systems reflect the biases of the people and management regimes that design them, and the biased data they are fed, and can create barriers to employment for people from protected groups, for workers whom employers determine are likely to exercise organizing and collective bargaining rights, and for people with arrest and conviction records. Because of this "bias in, bias out" problem, scholars caution that automated hiring processes “challenge the American bedrock ideal of equal opportunity in employment, as such automated practices may not only be deployed to exclude certain categories of workers but may also be used to justify the inclusion of other classes as more ‘fit’ for the job.” Moreover, unregulated algorithmic hiring creates risks of algorithmic repudiation where the same applicants experience repeated discrimination due to employers’ ability to retain or even share applicant profiles. A recent study by Cambridge University researchers found that these systems may “unintentionally entrench cultures of inequality and discrimination” and reproduce, rather than neutralize, biases.

For workers seeking jobs on digital labor platforms, on-demand jobs are allocated by secret algorithms. Job assignments, including the determination of which worker receives a job when more than one worker is awaiting work in the same location, may be determined by biased data, such as customer ratings.

Further, a study of job recruitment involving social media ad-targeting found that delivery-optimization algorithms on the company’s platform were perpetuating occupational segregation by gender and race. When researchers examined the audience for broadly targeted job positions, they found that the audience was 85 percent women for supermarket cashier positions and 75 percent Black for taxi driver positions.

2. **AWSM enables corporations to avoid accountability; this degrades wages and working conditions and fosters racial wealth and income inequality.**

Increasingly, corporations are turning to AWSM to manage and control workers even as they deny any responsibility for their wages or working conditions. AWSM empowers corporations to surveil workers more easily, collect data for secret algorithms, and use those algorithms to determine the terms and conditions of work. This growing reliance on AWSM enables corporations to mask their significant control even as they strip workers of core employment and labor rights such as the right to minimum wage, overtime, or the right to organize or be free from discrimination. Corporations have used AWSM to shed responsibility in at least two ways: first, by

---

4. Id. at 681-82.
falsely insisting that workers are independent contractors rather than employees; and second, by facilitating subcontracting to third parties over which they are able to use AWSM to maintain significant control.

AWSM is used to obscure corporate control and enable corporations to mislabel employees as independent contractors in underpaid industries with disproportionate numbers of Black and immigrant workers.

The corporate adoption of AWSM as a means of exerting non-transparent control is well documented. As the Federal Trade Commission noted in the context of digital labor platform workers:

[They] often do not have the information they need to know when work will be available, where they will have to perform it, or how they will be evaluated. Behind the scenes, ever-changing algorithms may dictate core aspects of workers’ relationship with a given company’s platform, leaving them with an invisible, inscrutable boss.8

This “invisible, inscrutable boss” may also use algorithmic pay formulas to personalize wages, which are neither negotiated nor transparent.9 Likewise, these bosses employ algorithmic rating systems that they use to discipline or terminate workers, leaving the workers at constant risk of sudden and potentially devastating economic consequences.10 The adoption of AWSM is particularly prevalent in corporations that use app-based labor platforms, where companies like Uber use gamified in-app reward systems, variable pay, and selective “surge-pricing” to effectively control where workers go, how long they work, and what kinds of trips they accept.

Yet many of the digital labor platform corporations that use AWSM as a hidden boss—to assign tasks, determine pay, and discipline or terminate workers—simultaneously insist that their workers are autonomous independent contractors, i.e., that the workers are in business for themselves.11 In so doing, they strip their workers’ of rights to minimum wage, overtime, workers’ compensation, unemployment insurance, health and safety protections, and protections from harassment and discrimination. They also shift the costs and risks of running a business to the workers and undermine the competition by reducing payroll costs. Corporate reliance on AWSM to facilitate mislabeling workers as independent contractors therefore undermines access to bedrock employment and labor law protections and social insurance programs.12 It also enables unfair competition and helps starve programs such as Medicare, unemployment insurance, and workers’ compensation.13


13 Leberstein, Why Misclassification Matters, supra n. 12.
Meanwhile, workers in industries where their employers’ independent contractor misclassification is prevalent—including those corporations that use AWSM to control the work—earn poverty wages and tend to make less than their employee counterparts. For example, a 2019 analysis by the Economic Policy Institute found that the average Uber driver’s wage was just $9.21 per hour after deducting fees and expenses, putting them in the lowest ten percent of wage earners, and earning lower than the minimum wage in many states and in the three largest cities. Similarly, a national study of workers hired via a digital labor platform (including delivery, ride-hail, and domestic workers) found that 1 in 7 workers earned less than the federal hourly minimum wage, and 30 percent of digital platform workers received a Supplemental Nutrition Assistance Program benefit, compared to 15 percent of employees in comparable service-sector jobs. Most recently, a study of the economic costs of misclassification to workers in 11 high-violation industries found, for example, that “a typical home health aide, as an independent contractor, would lose out on as much as $9,529 per year in income and benefits compared with what they would have earned as an employee.”

The impact of AWSM-supported misclassification of employees as independent contractors on communities of color is deeply disturbing. Persistent occupational segregation means that such misclassification disproportionately harms Black, Latinx, and Asian workers. As a group, workers of color—Black, Latinx, Asian/Pacific Islander, and Native American workers—are overrepresented in high-violation industries such as construction, trucking, delivery, home care, agricultural, personal care, ride-hail, and janitorial and building service occupations by over 40 percent; they comprise just over a third of workers overall, but make up between 47 and 91 percent of workers in these occupations. In digital labor platform work where AWSM is prevalent, Black and Latinx workers are overrepresented by 45 percent—more even than in more traditional misclassification-prone sectors. Thus, AWSM-supported independent contractor misclassification fosters a second-tier workforce comprised predominantly of workers of color stripped of core employment protections. Because it also comes with the significant wage and benefit penalties noted above, adoption of AWSM to perpetuate independent contractor misclassification also exacerbates racialized income and wealth inequities.

Lead firms in subcontracted work relationships use AWSM to exercise control while denying employer responsibility.

AWSM is not only used to enable corporations to mask control as they mislabel workers as independent contractors but is also used to control subcontracted work structures. A prime example is Amazon’s last-mile delivery model, in which Amazon uses subcontractor middle-managers to mediate its employment of some 275,000 delivery drivers, responsible for realizing the company’s two-day shipping guarantee. Although
delivery drivers are on the payroll of the subcontractor “delivery service partner,” (DSP) Amazon effectively controls the work through its smartphone app: setting daily routes, van color and Amazon logo signage, delivery quotas, and delivery deadlines for drivers by communicating through the app.21 Although directly employed by a DSP, drivers are required to sign “Biometric consent” forms allowing Amazon’s constant surveillance and related performance control via AI-powered cameras as a condition of work.22 The e-commerce giant installs these video cameras in the vans of the DSP drivers, sometimes using inaccurate data to penalize drivers or deny DSPs bonuses they may need to make vehicle repairs or enhance driver pay.23

In the wireless telecommunications industry, large carriers like AT&T, Verizon, and T-Mobile are increasingly outsourcing retail operations to third-party “authorized retailers.” A 2022 survey of workers at those authorized retailers revealed that large carriers often exert operational control over authorized retailers via digital performance tracking systems. Workers reported that, through those systems, carriers establish and frequently change performance benchmarks that determine pay for the commission-driven work.24

In short, AWSM has frequently been deployed by corporations to obscure their control and manage their workforces while insisting that their workers are independent contractors or outsourcing the work to third parties. By coopting the technology for their benefit, these corporations strip a disproportionately high percentage of Black and Latinx workers of bedrock rights and protections, degrade wages and working conditions and foster racial wealth and income inequality.

3. AWSM often increases barriers to organizing and bargaining collectively, particularly in industries with disproportionately high percentages of Black and immigrant workers.

As the National Labor Relations Board (NLRB) General Counsel recently cautioned, AWSM can infringe upon workers’ Section 7 rights under the National Labor Relations Act (NLRA). She noted in particular, “the potential for omnipresent surveillance and other algorithmic-management tools to interfere with the exercise of Section 7 rights by significantly impairing or negating employees’ ability to engage in protected activity and keep that activity confidential from their employer, if they so choose.”25

The use of AWSM to interfere with NLRA rights is not simply theoretical. Workers at Walmart discovered the company monitors online conversations about the union.26 HelloFresh tracks social media posts about the union by employees, and other corporations monitor work emails to identify what a former chair of the NLRB called

“pre-union activity, employee discontent.” Further, corporations have used AWSM to gauge the likelihood that workers would organize. For example, Amazon-owned Whole Foods used a combination of data concerning the poverty levels of workers’ neighborhoods, an index to measure the potential for racial solidarity, and measures of employee “loyalty” to identify stores where workers may support forming a union.

AWSM has also enabled corporations to maintain high levels of control over their labor force while denying labor rights under the NLRA. They do this through subcontracts that demand AWSM while denying their status as a joint employer. For example, just last month, drivers who were directly employed by a DSP at an Amazon fulfillment center in Southern California formed a union with the Teamsters, gaining voluntary recognition from the DSP. Amazon responded by announcing its intention to cut its contract with that subcontractor, effectively terminating the employment of the unionized drivers because they had exercised their Section 7 rights. Other lead firms that adopt AWSM to manage the work of their subcontracted labor may see this as a lesson and follow Amazon’s lead, adopting AWSM while denying responsibility for NLRA violations.

But these obvious efforts to chill organizing are not the only threat that unregulated AWSM poses. AWSM can also chill or undermine workers’ exercise of their legal rights to organize in myriad other ways.


corporate use of AWSM echoes slavery-based management and reinforces systemic bias

data-driven, algorithmic management is premised on quantifying work and work outcomes, and thus is readily applied to jobs where tasks are easily measured like retail, food service, warehousing, logistics, agriculture, hospitality, domestic work, and health care. Many of these industries have low levels of workers represented by unions and high percentages of Black and immigrant workers. Unregulated corporate use of AWSM can intensify the harms associated with unfairness and lack of transparency in the “at will” economy, undermining workers’ ability to speak up about mistreatment and perpetuating racial inequities. Low union density and increased surveillance can also be mutually reinforcing systems: suppressing workers’ power to insist on fair and transparent adoption and implementation of AWSM enables corporations to unilaterally and opaquey use it; and the constant pressure on workers to meet algorithmic demands under increased surveillance increases workers’ feeling of precarity and limits their ability to express power.

28 Daniel A. Hanley and Sally Hubbard, Eyes Everywhere: Amazon’s Surveillance Infrastructure and Revitalizing Worker Power, OPEN MARKETS (Sept. 2020), https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffe23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf.
30 Id. See also Unfair Labor Practice Charge Against Amazon Logistics, Inc., NLRB Board Region 31 (filed May 2, 2023), https://teamster.org/wp-content/uploads/2023/05/5323ULPChargeAgainstAmazon.pdf.
31 Nguyen, Constant Boss, supra n. 11.
This disempowering feedback loop is an extension of bosses’ long-standing use of work quotas and related distrust of Black and immigrant workers, whose worth was historically based on their ability to meet such quotas. It is a form of management rooted in the U.S. enslavement economy, where slavers ranked and attached monetary value to workers based on their productivity even as they surveilled based on racist beliefs about dishonesty, laziness, and trustworthiness. Using AWSM to code workers as good or bad mirrors the codes used to label Black and immigrant people in the carceral system (“high risk/low risk”), in the granting of social insurance (“worthy/unworthy”), and in access to the consumer credit markets (“excellent/good/poor”). Once attached to a worker, these codes can reify stereotypes about workers of color among management and determine when they are scheduled, what types of job tasks they are assigned, whether they are meeting standards, and whether they keep their job. If terminated as a result of such codes, quotas or algorithms, a workers’ access to critical unemployment insurance benefits may also be jeopardized.

Adoption of AWSM to code workers allows corporations to practice a form of just-in-time staffing where the algorithm itself determines who should be fired to minimize costs and maximize profits. And by pushing AWSM across companies and even industries, corporations can create a sense that always being watched is simply the normative condition at work, making it very difficult for employees to prove that any particular instance of surveillance was an effort to stymie protected concerted action.

**Constant and opaque use of AWSM increases worker perceptions of precarity and decreases solidarity among co-workers.**

In a unionized workplace, workers may be able to negotiate provisions in a collective bargaining agreement to address data collection, data sharing, and data use, and if a worker suspects unfair use of data to justify discipline or termination there would be a procedure in place to grieve the decision. But in most private workplaces without a recognized union, corporations can adopt AWSM in a “black box,” where workers have no voice or insight into how it was programmed, how it was put in place, or how the data is used. Trying to maintain algorithm-created productivity standards or understanding changing quota systems may leave workers too physically tired or demoralized to compare thoughts about working conditions. In some settings, productivity data may literally be used to pit workers one against the other; worker scores may be shared publicly on “leaderboards” comparing each worker’s progress toward the quotas to others.

---


40. Zickuhr, supra n. 11 at 21, *Workplace Surveillance*.


See also Nick Stat, *Amazon expands gamification program that encourages warehouse employees to work harder,*
Other forms of AWSM may discourage physical proximity of workers and therefore chill concerted activity. GPS trackers that allow employers to assess worker movements through a warehouse or a janitor’s progress in cleaning an office building can also reveal whether groups of workers are exercising their right to discuss conditions or potential unionization. High automated productivity quotas may discourage workers from taking legally permitted breaks where they could have encountered one another in a break room or a restroom. In other cases, worker awareness of corporate surveillance may compel organizing efforts to remain closely held, fostering a sense of wrongdoing when exercising legal rights. “If it’s too secret, too confidential, then it starts to feel illicit,” notes Saint Louis University School of Law Professor Matthew Bodie. “It’s like, oh, we shouldn’t be doing this.”

4. AWSM combines with other health and safety hazards to amplify unhealthy and unsafe work environments.

AWSM often combines with extant workplace hazards to exacerbate already dangerous working conditions. For example, warehouse workers subject to AWSM-related pressure to increase work speed do so in an environment already rife with multiple health and safety hazards. Workers toil in heat without training to recognize heat stress symptoms; they are exposed to chemicals in plastic with little information about potential health impacts; and they operate machinery with little or no personal protective equipment or training. These hazards, combined with AWSM-related pressure to meet quotas, dramatically increase the likelihood of injury or illnesses. Significant health and safety hazards are also common in underpaid industries such as warehousing, agriculture, and logistics. Because of occupational segregation, Black, Latinx, and immigrant workers are overrepresented in these more precarious, underpaid industries, therefore making injury rates higher for workers of color. Furthermore, hazards caused by increased pace of work quotas and surveillance are rooted in this country’s history of slavery, capitalism, and cotton production. Thus, Black and immigrant workers disproportionately experience the brunt of the legacy of quotas and increased pace of work through their overrepresentation in some of the most precarious industries.

Reliance on AWSM to increase pace of work can undermine worker health and safety.

AWSM poses a risk to workers’ health and safety when it is used to increase the pace of work. For example, regulators have noted that the high rates of serious injury at Amazon are directly attributable to the way that the


44 Constanz, supra n. 27, ‘They were spying’.


company manages its workforce using AWSM. And when Amazon temporarily suspended some of its productivity tracking and disciplinary policies in 2020, injury rates dropped significantly.

Meatpacking is another industry that has introduced AWSM in recent years. For example, some of the largest employers in that industry—which have a track record seeking to increase the speed of work even when it endangers the health and safety of frontline workers—have begun to use smart watch technology that "uses sensors to constantly collect data on the force, rotation, speed and directional movement of a worker’s arm as they perform the same motion over and over." These watches are marketed by third party vendors as tools to improve worker health and safety; however, they allow employers to much more closely track and surveil worker productivity and pose a potential risk to workers' health and safety, especially in the absence of regulatory standards limiting their use.

AWSM designed to monitor individual health risks may harm workers and enable discrimination in the absence of guardrails on data collection.

Current evaluation for heat stress, wildfire smoke exposure, and extreme cold exposure for workers is primarily based on broad environmental assessments and does not account for individual physiological responses to these inputs. In response, some health and safety experts have suggested wearable data-collection devices to individually monitor workers for possible illness or injury from exposure to environmental extremes. For instance, Chevron has implemented a skin patch that measures sweat levels and electrolyte loss while other companies are using a third-party sensor that measures heart rate, body temperature, and skin temperature. Individual biometric data could allow each worker to assess her own body's responses in real time and take action to protect herself from illness or injury. However, without regulation this kind of data collection and surveillance raises significant privacy and potential discrimination concerns.

While manufacturers tout the ability for supervisors to use aggregated data to determine the best times for rest breaks and claim that individualized data is only available to the individual worker, it is unclear how the data


Will Evans, Amazon’s warehouse quotas have been injuring workers for years. Now, officials are taking action, REVEAL NEWS, May 16, 2022, available at https://revealnews.org/article/amazons-warehouse-quotas-have-been-injuring-workers-for-years-now-officials-are-taking-action/.


collection might be regulated or how health information privacy rights like those in the Health Insurance Portability and Accountability Act can be enforced when employers are not subject to the privacy rule. Indeed, in a survey of safety engineers, the most often cited concern with the use of wearable data-collection, evaluation, and performance tracking devices worn by workers, in the workplace was protecting employee privacy and confidentiality. These respondents were concerned that even the perception of employer surveillance of such personal data could lead to ineffective use of the wearable devices and intentional lack of compliance by employees.55

To date, studies on the efficacy of these types of wearable devices as a health and safety tool have been largely limited to higher income countries and urban settings, occasionally on outdoor workers but often on younger students, athletes, and military enrollees. Significantly, among the studies that were addressing occupational heat stress, several found associations between sex, age, body mass index, and education and physical responses to heat stress.56 NELP is concerned that improper use of this data could facilitate discrimination against workers who are perceived to have pre-existing conditions or chronic health conditions or against workers with disabilities; because Black and immigrant workers often have less access to preventive care and experience some chronic health problems at a higher ratio than white workers, this type of health data collection could also have civil rights and Equal Employment Opportunity Commission implications or lead to violations of the Americans with Disabilities Act.57

At the same time, it is important for policymakers to recognize that other concerns such as data accuracy, worker access to data, and workplace safety may sometimes overshadow privacy concerns for workers. For example, a recent study showed that during the COVID-19 pandemic many essential workers indicated that health data transparency from their employer was a higher priority for them than their personal health data privacy.58

5. **AWSM is used to discipline and terminate workers without transparency or meaningful processes to contest decisions, degrading working conditions and potentially amplifying race inequities.**

Corporations also use AWSM to discipline or fire workers.59 Its use frequently decreases disciplinary transparency and limits workers’ access to human managers. For example, Amazon has “replaced its middle management and human resources workers with artificial intelligence to determine when a worker has outlived their usefulness and needs to be let go. There is no human to appeal to.”60 Workers have also reported having little recourse when AWSM systems have incorrectly or inaccurately disciplined them.61

Lack of access to a human manager can adversely affect workers’ experience of “organizational justice,” or “the role of fairness perceptions, e.g.,...the fairness of decision-making processes, and the fairness in interpersonal interactions.” Such experiences can degrade working conditions. Studies have shown that deficits in organizational justice itself can increase job stress and the risk of work-related musculoskeletal disorders.62

Corporate use of AWSM for discipline or termination can also magnify the existing power imbalance between employers and workers, especially in an at-will employment relationship. By providing second-to-second monitoring of workers’ actions, surveillance technologies can detect and record a momentary pause on the part of a worker and give employers the option of turning it into an infraction leading to discipline or termination. In this way, AWSM can greatly increase the volume of disciplinary actions, which has the potential to make it much more difficult for workers to contest unfair, discriminatory, or retaliatory disciplinary action or discharges.63

On the surface AWSM can lend the appearance of fairness in workplace discipline by subjecting every worker to a uniform interface with a non-human management system. In reality, aspects of AWSM have the effect of making discipline and firing processes more opaque, arbitrary, and unfair. Workers may have no ability to input or correct data, meaning that the data collected about their work performance may not reflect factors out of their control such as equipment malfunctions or a chance event.64 And when workers are disciplined incorrectly or inappropriately by AWSM for circumstances outside of their control, they may have little recourse or access to human decision makers.65

Finally, employer adoption of AWSM may also amplify existing inequities in workplace discipline. Research shows that employers scrutinize Black workers more than other workers and are less likely to give Black workers a chance to improve before terminating them.66 AWSM may exacerbate those dynamics by providing employers additional inexpensive and non-transparent means to engage in that kind of scrutiny.

6. AWSM facilitates unfair, unpredictable, and discriminatory pay.

As corporations turn to AWSM as a means of managing and controlling their workforces, they are also increasingly relying on algorithms to set wages, in many cases perpetuating wage discrimination based on biased customer reviews or through algorithms that are personalized to individual workers, thereby paying workers unequally for equal work.

For example, ride-hail drivers for corporations like Uber and Lyft are currently paid according to black-box algorithms that are opaque to both workers and consumers. Up until a few years ago, ride-hail companies set customer fares and worker pay with a relatively straightforward calculation, according to a fixed per-minute and


per-mile rate, and then sometimes with “surge” multipliers applied to the total. Then a couple years ago, Uber fully uncoupled customer fares and worker pay, setting both according to complex and invisible algorithms, meaning that there is no longer any necessary connection between what a customer pays and what a driver is paid.

One result has been a pattern of skyrocketing consumer fares while driver pay continues to fall or stagnate. Another result has been that work as a ride-hail driver—or on-demand work more generally—is increasingly unstable and unpredictable. Workers whose wages are determined by an obscure, complex system may make dramatically different amounts on different days for the same amount of work. Therefore, corporate adoption of AWSM increases precarity; workers are unable to predict or understand their constantly changing, frequently declining compensation, and many struggle to plan financially.

More troublingly, because driver pay is not fixed according to any set of objective criteria, company algorithms can pay two drivers different amounts for identical trips. A recent video uploaded to YouTube, by the hosts of a popular show about working as a ride-hail driver demonstrates what this looks like in practice: two Uber drivers, sat next to each other on a couch at one of their homes in Chicago, log onto the app at the same time and watch as they are presented identical trips at different fares. Because those algorithms are tightly held, it is currently impossible for anyone outside of Uber to understand what determines the different fares. But, as one scholar exploring this issue has put it, it seems highly likely that on-demand companies like Uber are “offering vulnerable workers lower wages based on their willingness to accept work at lower prices.” In other words, AWSM threatens to pave the way for a new labor management practice: using individualized worker data to identify exactly the wage at which a given worker will accept work, and then paying them that amount. The upshot is that poor workers, Black workers, immigrant workers, and women workers may be paid less for doing equal work.

And by no means are these trends limited only to ride-hail workers. As companies in industries like retail, food service, and medical care adopt the labor management technologies pioneered by Uber, the practice of algorithmic wage discrimination is spreading.


70 Id. at 7.

71 2 Uber Drivers: Same Requests DIFFERENT PAY! You Won’t Believe This!, THE RIDESHARE GUY YOUTUBE CHANNEL (Mar 1, 2023), available at https://www.youtube.com/watch?v=UADTiL3S67I.

72 Dubal, supra n. 69, at 40 ("As a labor management practice, algorithmic wage discrimination allows firms to personalize and differentiate wages for workers in ways unknown to them, paying them to behave in ways that the firm desires, perhaps as little as the systemic determiners that they may be willing to accept."); Id. at 6.


74 For more information on this company, see Nicky Godding, Oxford Tech Raises £9 Million for ‘Uber for Hospitals’ AI Platform, BUSINESS INNOVATION MAGAZINE, May 21, 2020, available at https://www.businessinnovationmag.co.uk/oxford-tech-raises-9-million-for-uber-for-hospitals-ai-platform/.
across the economy could be paid according to opaque and personalized algorithms that obscure systemic wage discrimination along protected lines of race and gender.\footnote{Teachout, supra n. 9, \textit{Algorithmic Personalized Wages} ("Uber drivers' experiences [of wage discrimination] should be understood not as a unique feature of contract work, but as a preview of a new form of wage setting for large employers: individualized pay, schedules, benefits, and individualized behaviorally based incentive structures.")}

7. **Policy recommendations to address the harms of unregulated corporate adoption of AWM.**

As detailed above, corporate adoption of AWM is creating new barriers to employment (both finding and keeping jobs), employer accountability, workplace democracy, health and safety, and fair compensation, particularly for Black, immigrant, and women workers. Mitigating the risks and harms posed by corporate AWM practices will require deliberate worker engagement, ongoing evaluation, updates to administrative policies and legislation, and significant investments in enforcement.

1. **\textit{The Administration should support policies that expand worker voice and worker power, which are fundamental to eliminating the harmful effects of AWM.}**

Workers must have a voice in the adoption of AWM at work and play a central role in evaluating its use. They should have institutional power to develop and enforce policies that eliminate or minimize the AWM's harmful impacts.

- Unions provide workers with a voice on the use of AWM by their employers.\footnote{Kresge, \textit{Union Collective Bargaining}, supra n. 41.} Recognizing this, the White House should work with Congress to advance the Protecting the Right to Organize Act to expand organizing and collective bargaining protections. Workers should be able to bargain freely over the adoption, use, limitations of, as well as protections from, AWM in any contract.
- To help ensure AWM is not used to silence organizing, the NLRB should formally adopt the framework established by the General Counsel’s memo on unlawful electronic surveillance and automated management practices. Specifically, the Board should adopt a presumption that the use of AWM is a violation of privacy and of the right to organize, absent compelling justification.\footnote{See NAT'L LAB. REL. BD. memo, supra n. 25, at 8.}
- The Administration or the NLRB should consider adopting rules to require employee consent to electronic surveillance and can look to state law models.\footnote{See, e.g., California law rendering it a misdemeanor to use electronic tracking of an employee without her consent. Kendra Rosenberg, \textit{Location Surveillance by GPS: Balancing an Employer’s Business Interest with Employee Privacy}, 6 WASH. J. L. TECH. & ARTS 143, 149 (2010).}

2. **\textit{The Administration should establish ongoing evaluation on corporate use of AWM.}**

Given the skyrocketing, opaque, and largely unregulated adoption of AWM, the Administration should develop policies and procedures to ensure regular and transparent evaluation of its impact on workers.

- The BLS should field the CPS module mentioned above regularly to ensure that the Department of Labor (DOL) and worker advocates stay abreast of AWM impacts on workers.
- To account for the fact that workers may not be privy to the extent of their employers' use of AWM, the Administration should work with the BLS, the DOL Inspector General, and the Commerce Department to survey and audit businesses regarding their adoption and use of AWM. Following the examples of some states, the Administration should explore requiring regular and public disclosure of what information is...
collected, where it is stored and for how long, how it is used, and if it is shared.\textsuperscript{79} Relatedly, because AWSM is currently developed and implemented largely in secret, robust worker notice and transparency measures should be developed.\textsuperscript{80}

- The White House should work with the Commerce Department to examine the patenting process and to ensure that the worker impact assessments are incorporated.
- The Administration should work to ensure that patents for technologies with workplace applications ensure jobs aligned with the DOL’s Good Job Principles.

3. \textit{The Administration should establish a Privacy and Technology Division at the DOL to help protect workers from the harms of AWSM.}

NELP supports the proposal put forth in the Stop Spying Bosses Act of 2023 (S. 262) to establish a Privacy and Technology Division at the Department of Labor to enforce and regulate workplace surveillance, with annual reporting to Congress on workplace surveillance and employer actions to control workers, including how and to what extent AWSM systems harm workers.\textsuperscript{81} The White House should work with Congress to advance this legislation which would additionally require any employer engaging in surveillance and collecting data on employees or applicants to disclose such information in a timely and public manner; prohibit employers from collecting sensitive data on workers such as off-duty data collection or data collection that interferes with organizing; and create robust rules around the usage of automated decision systems.

4. \textit{The Administration should issue guidance and invest in enforcement to eliminate the use of AWSM as a tool for evading employer accountability.}

Many of the harms inflicted by widespread corporate adoption of AWSM are the result of the way AWSM enables the violations of other laws, particularly how it helps strip workers of core employee and labor protections. Accordingly, NELP recommends that the Administration use its existing authority to promulgate guidance and use strategic enforcement to protect and restore employee rights. NELP recommends the following:

- The DOL’s proposed rule on independent contractor classification under the Fair Labor Standards Act (FLSA) should be finally promulgated to ensure broad access to minimum wage and overtime protections Congress intended under the FLSA. The DOL’s express consideration of surveillance and technology should be retained and strengthened in the final rule to specifically identify \textit{algorithmic control} as a form of technological control weighing in favor of employee status. The rule should recognize that control over the work, even if exercised by algorithmic management on a smartphone or electronic surveillance, is probative evidence of an employment relationship.
- The DOL should issue guidance clarifying what constitutes “compensable time” for individuals working on labor platforms that currently use AWSM to deny pay for a significant portion of workers’ time, such as when a ride-hail driver is returning from a drop off or waiting for a passenger.\textsuperscript{82}
- The NLRB’s rulemaking to restore “joint employer” accountability under the NLRA should address the role of AWSM in preventing or chilling worker organizing. It should recognize the use of AWSM as an indicator of an employment relationship and restore accountability for labor law violations by corporations—like Amazon—that use AWSM to control their subcontractors and workers throughout

\textsuperscript{79}Connecticut and Delaware both require disclosure to employees of surveillance practices. \textit{See} Conn. Gen. Stat. \S\ 31-48d(b)(1); Del. Code Ann. tit. 19, \S\ 705.


their fissured workforce. Specifically, the Board should clarify that employers’ use of AWSM is indicia of an employer’s “authority to control” and suggests direct or indirect “power to control” under the NLRA.

5. The Administration should establish standards for disciplinary transparency and fairness for federal contractors using AWSM.

The enormous power of AWSM should be decoupled to the greatest extent possible from the processes of workplace discipline and termination to guard against abuses and reduce the increased power imbalance between workers and employers. Curbing the use of AWSM for the purposes of discipline and termination, together with greater protection against abrupt and arbitrary firings, would help diminish harm to workers and the erosion of job quality. The Administration should, at a minimum, begin this work with its federal contractors, by implementing the following standards:

- Federal contractors should be prohibited from using the most invasive forms of AWSM (such as biometric monitoring or apps installed on personal devices) for the purposes of discipline and termination. These employers should also be required to meet standards of fairness and transparency when using AWSM to discipline or terminate workers. Such standards could include requiring employers to use the least invasive surveillance method available and to provide justification and third-party certification for any surveillance they plan to use for the purposes of discipline or termination. These provisions are included in a bill recently introduced in the New York City Council.83
- Federal contractors’ use of electronic monitoring in relation to productivity tracking and pace of work should be restricted. Measures could include, for example: banning continual “time off task monitoring” allowing it only as part of a periodic pre-announced performance review;84 and limiting the time increments in which quotas can be measured, i.e., allowing for quotas to be measured by the day, and not by shorter increments of time such as the hour or minute.
- The Administration should require federal contractor disclosure of performance standards and fair processes for discipline and termination. Any attempt to regulate the use of electronic monitoring will have a limited effect in the absence of baseline legal protections related to discipline and termination. For example, policies that require disclosure of AWSM use, access to data collected by AWSM, or that impose broad blanket bans on AWSM (such as the proposed Stop Spying Bosses Act of 2023—S. 262 that bans surveillance that threatens employees’ mental or physical health) will be less effective in an at-will employment context. If enacted in the absence of required disclosure of performance standards, disciplinary policies, warnings, fair processes, and reasons for discharge, employers will continue to use AWSM in opaque ways that leave workers little recourse when they are unfairly discharged based on data from AWSM. As such, the Administration should consider establishing “just cause” protections for all employees of federal contractors.85 The Administration should consider how best to expand these federal policies to the private sector in keeping with its Good Jobs Principles and for the benefit of all workers.

* * *

As detailed above, NELP is concerned with unregulated and opaque corporate adoption of AWSM and its impacts on employment, compensation, health and safety, discrimination, and worker power, particularly for Black and immigrant workers. Corporate adoption of AWSM without worker input, voice, transparency, and evaluation threatens to erode employer accountability, increase barriers to collective action, amplify unsafe or unhealthy working conditions, facilitate unpredictable and discriminatory pay, increase racial income inequality, and leave

83 Wrongful Discharge from Employment, N.Y. City Council, Int. 0837-2022, Committee on Consumer and Worker Protection, available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=5958217&GUID=44D72CEC-FE82-4A43-BA31-4BB15FBC15EB&Options=ID%7CText%7C&Search=s%3D%3D.
84 Id.
workers without recourse for unfair and opaque discipline or termination. NELP appreciates the opportunity to comment on this important topic.

Sincerely,

Anastasia Christman, Senior Policy Analyst
Sally Dworak-Fisher, Senior Staff Attorney
Nicole Marquez, Director of Social Insurance
Daniel Ocampo, Legal Fellow
Maya Pinto, Senior Researcher and Policy Analyst
Irene Tung, Senior Researcher and Policy Analyst
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0182
Comment on FR Doc # 2023 12995

Submitter Information

Email: [REDACTED]
Organization: TechNet

General Comment

See attached file(s)

Attachments

FINAL TechNet response to OSTP RFI on AI in Workplace
June 29, 2023

Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, D.C. 20504

To Whom It May Concern:

TechNet appreciates the opportunity to respond to the Office of Science and Technology Policy's (OSTP) request for information on automated systems use in the workplace. Our members represent many of the leading artificial intelligence (AI) developers, researchers, and deployers of automated systems.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than 4.5 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

AI and machine learning (ML) are transformational technologies that have the potential to revolutionize how we live and work and help us solve the most significant challenges of our time. AI and ML can enhance productivity, democratize and expand access to important services, and improve product innovation.

North America currently leads the global AI market — in 2021, the global AI industry was valued at $59.67 billion, and North America accounted for about 43 percent of overall global revenue. However, our international competitors are working quickly to overtake our lead; spending in China’s AI industry is forecast to hit $14.75 billion in 2023, accounting for about 10% of the world total. China also currently leads in AI adoption, with 58% of companies deploying AI and 30% considering integration. In comparison, the United States has less than half this adoption rate, with 25% of companies utilizing AI and 43% exploring its potential applications. Industry and government must work together to ensure our nation remains the global technology leader.

TechNet believes that AI systems must be designed, developed, and implemented responsibly and in a way that allows the United States to maintain its lead in innovation and builds consumer trust in AI. There are a range of concerns to consider, including but not limited to privacy, transparency, data veracity, bias, security, and workforce. Designers, developers, deployers, and users of AI systems are working to ensure appropriate oversight and accountability; continually monitor and assess the need for improvements related to safety, fairness, and trustworthiness; protect against malicious activity; and address flawed data sets or assumptions. AI regulations should focus on mitigating known risks and providing developers with clear metrics to review their systems.

**Existing Legal Protections**

It is important to note that the use of AI in furtherance of unlawful behavior is already prohibited and is actionable under existing laws, even in the absence of AI-specific regulation. For example, many existing anti-discrimination laws apply to AI models in important areas, including employment and the workplace (i.e., Title VII of the Civil Rights Act of 1964, the National Labor Relations Act, and the Americans with Disabilities Act).

Several federal leaders have stated their intent to use existing laws to regulate AI; for example, National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo has stated that she will “… apply the [National Labor Relations] Act to protect employees from intrusive electric monitoring and automated management practices...”. ³ On April 25, the Consumer Financial Protection Bureau, the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Federal Trade Commission issued a joint statement outlining how their existing enforcement authorities apply to automated systems. ⁴ Additional oversight in these areas should not be unnecessarily duplicative or create inconsistent or conflicting standards.

TechNet members comply with existing legal protections, including existing privacy and anti-discrimination laws. The use of automated technologies in the workplace does not fall outside of the scope of these legal protections. Accordingly, TechNet members adopting AI technology do so cautiously and only after rigorously assessing the benefits and risks of implementation.

**Enhancing Safety**

Several TechNet members use automated tools to provide navigation, routing, and transportation safety assistance to users, independent contractors, and employees. NHTSA projects that an estimated 42,915 people died in motor vehicle traffic crashes in 2021, a 10.5% increase from the 38,824 fatalities in 2020. This projection is the

---


highest number of fatalities since 2005 and the largest annual percentage increase in the Fatality Analysis Reporting System’s history.\(^5\) TechNet agrees with Transportation Secretary Pete Buttigieg, who stated that “[t]he rising fatalities on our roadways are a national crisis; we cannot and must not accept these deaths as inevitable.”\(^6\)

Many members utilize telematic services to improve the efficiency and safety of their fleets. Research has shown that these services can decrease risky driving practices. Cambridge Mobile Telematics, the world’s largest telematics service provider, has shown that its Hard Brake Alerts have helped reduce hard braking by 14%, and that of the drivers who have experienced Hard Break Alerts, 72% said the alert positively influenced their driving behaviors. Hard Brake Alerts are also an optional feature — drivers can opt out at any time.\(^7\) As tens of thousands of Americans continue to die on our roadways every year, companies are working to deploy tools to keep their employees and independent contractors safe as they go about their work.

AI-empowered technologies can also keep employees safe from incidents beyond the roadways. Samdesk, a global crisis detection platform, works with several companies to provide Real-Time Safety Alerts in the event of emergencies.\(^8\) This system reviews public data sets to spot disruptive events and send early warning alerts and insights, often ahead of traditional news and crisis monitoring tools. This can allow companies to alert employees, independent contractors, and users about the incident, suspend operations, avoid the impacted area, and stay out of harm’s way.

**Improved Cybersecurity**

Automated tools are also being deployed to actively protect employees’ devices from cybersecurity threats. With fast-evolving cyberattacks and the multiple devices individuals now utilize today, AI and machine learning (ML) can help to keep cybercriminals at bay, automate threat detection, and respond more effectively than conventional software-driven or manual techniques. By using sophisticated algorithms, automated systems are being trained to detect malware, run pattern recognition, and detect even the most minute behaviors of malware or ransomware attacks before they enter the system. Ransomware attackers extorted at least $765.5 million from victims in 2021, and the real number is expected to be much higher.\(^9\) Many of these cybercriminals are working on behalf of America’s hostile competitors. Earlier this year, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on how the Democratic People’s Republic of Korea (DPRK) state-sponsored ransomware

---


was targeting America’s healthcare systems. These extorted funds then go on to support the development of additional malicious technologies to target American and allied entities. Automated tools can help protect public and private institutions, Americans’ personal data, and our economy writ large from cybercriminals.

**Supporting Employees with Advanced Tools**

Automated systems are being deployed in workplaces across the country to help free employees from rote and inefficient tasks so they can focus on creative outputs. Several of our members utilize automated tools to assist with scheduling, which can ensure more experienced managers are on the same shift as new employees for mentoring, coordinating predictive maintenance for equipment, or when additional orders for needed supplies should go out. While a human could organize these services, by automating these operations, employees are able to make decisions more quickly and go about their workday in a more efficient manner. We are seeing that AI-driven tools enable larger, more integrated teams because entities can coordinate and collaborate more effectively. According to a study by MIT Sloan, employees that are empowered by AI feel more competent in their roles, more autonomous in their actions, and more connected to their work, colleagues, partners, and customers. Only 8% of the global survey respondents were less satisfied with their jobs because of AI. When reviewing the impact of automated tools in the workplace, TechNet urges OSTP to consider the wider context of these systems’ impact on employees’ well-being in their careers.

**Scoping**

We also want to highlight the importance of clearly defining artificial intelligence. Two key documents that policymakers repeatedly point to, the White House’s Blueprint for an AI Bill of Rights and NIST’s AI Risk Management Framework, utilize different definitions of AI. While both documents offer voluntary, non-binding guidance, these differing definitions — both issued by the same administration — can send confusing messages to businesses that develop and deploy AI. We advise the use of the NIST AI RMF’s definition of an AI system for two reasons: 1) the RMF was developed through close coordination with the experts from the AI community, and 2) it was adapted from existing AI industry definitions. Adopting the NIST AI RMF definition across the government will help provide greater clarity for the public’s understanding of AI systems.

---

12 The AI RMF defines an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.
The Need for a Federal Privacy Law

We also want to take this opportunity to highlight the need for a federal privacy law, which would allay concerns about the harm to consumer privacy from the use of AI. In the RFI, OSTP makes repeated mention of the importance of protecting Americans’ privacy. The passage of a federal consumer data privacy law should be a part of or pass concurrently with AI-focused policy, as privacy legislation would apply to and mitigate some risks to consumers stemming from using AI systems. A federal privacy law will help consumers understand their rights relating to the data used to inform automated systems and will assist developers in knowing their liability when managing large datasets. By having a clear national framework, we can help build trust in AI systems deployed across the United States utilizing the same standards when it comes to consumer privacy.

TechNet has long urged policymakers on Capitol Hill to craft a federal privacy law that protects consumers and provides businesses with certainty about their responsibilities. The current and growing landscape of state privacy laws has created a patchwork of laws, standards, and obligations that confuse consumers and hurt our nation’s innovators, especially our small and medium-sized businesses. Costs from 50-state privacy laws could exceed $1 trillion over ten years, with at least $200 billion being paid by small businesses.14 A federal privacy law will help consumers better understand their privacy rights and avoid the confusion resulting from differing policies state-to-state.

Congressional action is the best approach to a federal privacy law because Congress can expressly preempt state laws and ensure that authorities with relevant expertise are responsible for enforcement. This is also an issue of bipartisan interest; a Morning Consult survey found that 86 percent of Democrats and 81 percent of Republicans said Congress should make privacy a “top” or “important” priority.15 TechNet is pleased that Congress has recently demonstrated a willingness to address this challenge and is making real progress toward passing bipartisan federal privacy legislation. We are hopeful this momentum continues and culminates in a uniform, coherent national privacy framework.

Conclusion

The federal government must avoid blanket prohibitions and overly prescriptive requirements on AI, ML, or other forms of automated decision-making. With the increased interest in AI due to the popularity of publicly accessible generative AI systems, there has been a discussion of policies that would inhibit the United States’ ability to continue leading in this important technology. These suggestions have

---

15 Sabin, Sam. “States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data.” Morning Consult. April 27, 2021. https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/?mkt_tok=ODUwLVRBQS01MTEAAAF8tGX5mckivVTqDBnO2P6uk8SwNzpikG6iODLZbMUSXoCz_rBTKebgwsCEXLO1x0rfXmhJBFrEj02zoCIquwy_kXz5nl02m-CJADuAAR7j8c.
included a proposal to place a six-month ban on AI development,\textsuperscript{16} which would merely lend additional time to foreign competitors to gain an advantage over American AI development. Any restrictions on automated decisions should be risk-based and focused on responding effectively to specific actual harms while allowing for advancements in technology and innovation. A risk-based regulation allows for application across industries and will help future-proof policies as this technology continues to develop. TechNet advocates for requirements of manual alternatives to be tailored to the known risks associated with each specific use case. Furthermore, TechNet strongly urges the development of AI regulations in collaboration with sector experts who possess deep knowledge of the use cases where the technology is being deployed. This collaboration will help ensure that regulators have the necessary expertise to effectively address the unique challenges presented by each sector’s AI applications.

We look forward to working with you on AI policy and appreciate the opportunity to discuss this innovative technology. Thank you for your consideration of our perspective on this important issue.

Sincerely,

Carl Holshouser
Senior Vice President

My name is Khali Jama. I am an immigrant from Somalia, a mother of two, and a member of The Awood Center, where the East African Community learns, defends our rights at work, and builds East African worker power. We are a worker led organization dedicated to educating, organizing, developing leadership and mobilizing to improve the economic and political life of the community and all working people. Please see the attachment where I share my experiences with surveillance and automated management while working at an Amazon warehouse in Minnesota. Thank you for this opportunity.
My name is Khali Jama. Thank you for this opportunity to share my experiences with surveillance and automated management while working at an Amazon warehouse in Minnesota. I am an immigrant from Somalia, a mother of two, and a member of The Awood Center, where the East African Community learns, defends our rights at work, and builds East African worker power. We are a worker-led organization dedicated to educating, organizing, developing leadership and mobilizing to improve the economic and political life of the community and all working people.

I thought Amazon was a safe place to work at until I started working there last year as a stower and a water spider. I noticed the majority of my coworkers on my shift, Latinas and Somalis, don’t always speak English or know their rights. I see a lot of people who break their backs working at Amazon because they have bills to pay and families to take care of. Amazon’s rate and TOT/ time off task system, Amazon’s pressures, and the fear they put in us are the reasons workers are getting injured. It’s not fair to the employees who work there, and it is all made possible because of their surveillance.

I have never in my life experienced what I experienced at Amazon. Sometimes the workload is very heavy, and you are working 10 hour shifts. Sometimes we have to work up to 12 hours per day, five days a week, whether we like it or not. If you don’t work those 12 hours, they will fire you. Unless you’re ill and have a note from the doctor, or unless you have a good reason for not coming in. They want you to work at a certain speed. When people cannot work at that speed, managers will come and harass you, telling you your rate is down. They don’t care if you’re sick, they don’t care if you’re not feeling well, you have to make rate. Let’s say I’m feeling ill or have a muscle ache because of the load of work, they still want you to make 250 each hour. Some of those loads are huge. If you’re still not at that speed that they want you to be, they’ll come and talk to you a second time. The third time, you get a write-up, and you’re fired through an app.

One of the reasons there are so many injuries is the rate, the speed, and the fear. And we know Amazon’s injuries are underreported from the recent OSHA citations in several states.

they’ll say I have too much TOT. From certain stations, it takes seven minutes to walk to the bathroom. We know this because since Amazon tracks us, we have to track our time too. Each floor has two bathrooms, so if it’s busy, and you go to the next one, the minutes add up, but Amazon does not care. Every day we’re afraid to get written up, sometimes you don’t even know what you can get written up for. You frequently hear someone got fired because of TOT or going over their allowed time off. Every Sunday we have new workers in the warehouse.

but I had to come in to work because I didn’t have unpaid time or vacation. I cannot continue to work another six hours and I don’t have any time off.” The managers tried to help but they didn’t have any power, they said their hands were tied. I went to HR, but she said there’s nothing I can do. What does it take for me to get a day off?
I was sent to a place called Amcare where they don’t do much for you. They just tell you to take this pain killer. I got scared because they offered me a pain killer without asking me if I have any allergies. Otherwise, Amcare does not do anything for you. They wouldn’t let me rest unless my back was broken or I had a bad injury. Then they said I couldn’t go back to work unless I had a doctor’s note.

Afterwards, I asked for my incident report, but Amazon didn’t have it, they didn’t have a record of me going to Amcare. How can you not have a report after I spent an hour and a half arguing to go home? I ended up leaving to get the care I needed because I know my rights, but there’s people who are afraid to lose their jobs, because Amazon puts that fear in them so people won’t even go to the bathroom.

They are constantly tracking you, but when you have questions, when you want to leave, there’s no one to talk to. There’s no manager, no PA. I always say what’s the point of having a manager who you cannot talk to, and when you finally find someone, they say, “my hands are tied.” You go to HR, they say go to the app. But my coworkers don’t all speak English, sometimes they don’t know how to read and write in English but Amazon hired them. I’ve been pushing for Somali translators on my shift. With Amazon, you don’t get to talk to people, you get to deal with an app that tells you what to do or what not to do. I don’t understand their system and I speak the language. I understand my rights and I’m still confused. So imagine the people who don’t know their rights. Because the majority doesn’t know how to use this automated technology.

If you’re late one minute, they’ll take a whole hour away from you, and that’s how you end up with no time off. If you get sick today and call Amazon, they will tell you to take a leave of absence. They won’t reply to that leave request for another 72 hours and that’s how a lot of people lose their jobs. When you apply for a leave of absence, you expect they’re going to understand why you didn't go back to work. The next thing you know you are fired. You don't even know. No one tells you anything. You come to work, and you can't get in, because you've already been fired. In one week, they fired over 25 people. Every single night I go in there and someone gets fired because of their TOT, their rate is low, or they have negative hours.

I go to work and try my best, but they don’t care. They usually say, you can leave if you want. They say, you don’t have to be here. It’s not fair for Amazon to treat us this way, as hard as we work, as much pressure we work under. We all do our part, we love working, and we want the government to see what Amazon is doing is not fair.

The most important thing is knowing you’ll be safe when you come to work. I’m a mother of two kids in college. At the end of the day, I want to be able to go home to my family without my back aching or living in fear of being told my rate is low when I go back the next day. That’s why I have organized with my coworkers in different warehouses for safer working conditions at Amazon, and I have advocated for the Minnesota Warehouse Worker Protection Act. We need stronger protections and for everyone to know their rights.
**General Comment**

I feel that this is deeply invasive and disrupts an employee's bare minimum sense of privacy. It also offers a multitude of opportunities for employers to abuse workers through slanted documentation that can be used to justify retaliatory terminations or simply create psychologically distressing work environments. If a performance issue can't be evaluated by managerial staff in normal employee reviews with all the context that that human lends provides, than it shouldn't be part of the employees evaluation.
Please find a comment from Partnership on AI attached, along with the reports it references.
The Partnership on AI Response to the Office of Science and Technology Policy’s Request for Information: Automated Worker Surveillance and Management

Document ID OSTP_FRDOC_0001-0004
Federal Register Number 2023-09353

June 26, 2023
About Partnership on AI

Partnership on AI (PAI) is a non-profit partnership of academic, civil society, industry, and media organizations creating solutions so that AI advances positive outcomes for people and society. PAI studies and formulates sociotechnical approaches aimed at achieving the responsible development of AI technologies to advance the public’s understanding of AI and to serve as an open platform for discussion and engagement about AI and its influences on people and society. Today, we connect 105 multi-stakeholder partners in 17 countries to be a uniting force for the responsible development and fielding of AI technologies.

PAI develops tools, recommendations, and other resources by inviting diverse voices from across the artificial intelligence (AI) community and beyond to share insights that can be synthesized into actionable guidance. We then work to promote adoption in practice, inform public policy, and advance public understanding. We are not an industry or trade group nor an advocacy organization. We aim to change practice, inform policy, and advance understanding.

The information in this document is provided by PAI and is not intended to reflect the view of any particular Partner organization of PAI. The comments provided herein are intended to provide evidence-based information into the OSTP's deliberations as opposed to advocating for any particular regulatory approach or action.
Partnership on AI’s insights on job quality impacts of automated worker monitoring systems
(in response to Question 4.b, “What data and evidence exist on the impact of automated worker surveillance and management systems on workers?”)

In September 2022, Partnership on AI (PAI) released a report titled “AI and Job Quality: Insights from Frontline Workers.” The report is based on an international qualitative study of on-the-job experiences with automated systems and documents the experiences of warehousing workers in the US, data-processing workers in sub-Saharan Africa, and customer support workers in India. All of the artificial intelligence (AI) systems that research participants interacted with were intended to assist with work tasks. This included monitoring workers’ on the job activities, such as physical movements, speech, clicks, and keyboard inputs.

PAI identified five common themes in workers’ experiences with workplace AI:

1. **Workplace AI’s harms are not new or novel.** They are repetitions or extensions of harms from earlier technologies and, as such, should be possible to anticipate, mitigate, and eliminate, often under existing laws, regulations, and agencies. Still, these systems can accelerate the scale and depth of harms beyond existing enforcement capacities and capabilities. Addressing the expansion of existing harms may require commensurate, substantial expansions of agency and regulatory body funding and headcount, and increased incentives/penalties for compliance.

2. **Current implementations of AI often serve to reduce workers’ ability to exercise their human skills and talents.** Skills like judgment, empathy, and creativity are heavily constrained in these implementations. To the extent that the future of AI is intended to increase humans’ ability to use these talents, the present of AI is sending many workers in the opposite direction.

3. **Empowering workers early in AI development and implementation increases the opportunities to attain the aforementioned benefits and avoid the harms.** Workers’ deep experience in their own roles means they should be treated as subject-matter experts throughout the design and implementation process.

4. **Executive and managerial decisions shape AI’s impacts on workers, for better and worse.** Organizations that purchase and use workplace AI hold many of the critical procurement and implementation decisions that shape worker experience hence their actions are no less important to determining AI’s ultimate impact on workers than those of AI-creating companies.

5. **Workers have a genuine appreciation for some aspects of AI in their work and how it helps them in their jobs.** Where automated monitoring contributes to their achievement of their workplace goals (e.g., working with less physical strain, providing
useful optional coaching, completing work tasks more accurately or efficiently) without otherwise degrading their experience (e.g., through punitive and inaccurate performance assessment systems, increased job intensity, implicit encouragement to skip breaks, or chilling conversations about working conditions), workers usually welcome the technology.

The full report is available at https://partnershiponai.org/paper/ai-and-job-quality/.
PAI’s Guidelines for AI and Shared Prosperity

(in response to Question 5.a, “What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers’ rights?”)

In June 2023, PAI released the Guidelines for AI and Shared Prosperity: a set of tools to inform the design and development of workplace AI systems to protect workers’ rights and well-being. The Guidelines are based on the insights from frontline workers published in PAI’s AI and Job Quality report. The Guidelines were developed under the guidance of a multidisciplinary Steering Committee, consisting of senior leaders from the labor movement, technology industry, civil society, and academia.

The Guidelines seek to comprehensively address AI’s impacts, including those related to automated worker monitoring and surveillance. They offer two tools:

1. **A high-level Job Impact Assessment Tool**, which includes:
   - Signals of Opportunity indicating that an introduction of a given AI system into the workplace may improve workers’ well-being
   - Signals of Risk indicating that introduction of an AI system may harm workers

2. **A collection of Responsible Practices and Suggested Uses** to help minimize the risks and maximize the opportunities to improve workers’ well-being with AI, tailored for specific stakeholder groups:
   - AI-creating organizations
   - AI-using organizations
   - Labor organizations
   - Policymakers

When using the Guidelines, we encourage stakeholders to:

- **Avoid interpreting the presence of signals of opportunity as “offsetting” the presence of signals of risk.** In recognition that benefits and harms of AI are usually borne unevenly by different groups, the Guidelines strongly oppose the concept of a “net benefit” of workplace AI systems. An effective mitigation strategy should be developed for each risk an AI system is expected to pose to workers. If effective mitigation strategies for a given risk are not available, meaningful changes must be made to the AI development and use plans.

- **Make sure workers are engaged in the design and deployment of AI systems, as well as the development of risk mitigation strategies.** In cases where one group of workers uses an AI system (for instance, uses an AI monitoring tool to assess the performance of their direct reports) and another group is affected by that AI system’s use (in this example, the direct reports), we suggest giving highest consideration to affected workers and/or the workers with the least decision-making power in the situation (in this example, the direct reports rather than the supervisors).
PAI’s Policy Recommendations

We encourage governments to integrate the Job Impact Assessment steps or similar into existing or emerging AI-related standards, risk management frameworks, and conformity assessments to encourage AI-creating and AI-using organizations to assess and disclose their anticipated impacts on workers and abide by Responsible Practices suggested by the Guidelines for AI and Shared Prosperity or similar. We also encourage governments to adopt the Guidelines or similar in their own employment contexts, and to require recipients of major economic development funding and of major government contracts to do the same.

We encourage disclosure of the presence of the below risk signals associated with automated worker surveillance and management systems.

It is a risk to workers if an automated system can intentionally or unintentionally be used to:

- Accelerate the pace of task completion without meaningfully changing resources or tools available to accomplish the tasks
- Reduce workers’ schedule predictability
- Induce workers to shorten their break time
- Increase overall difficulty of tasks (without commensurate compensation or adjustments to workload)
- Monitor something other than the pace and quality of task completion
- Reduce workers’ autonomy, decision-making authority, or control over how they complete their work
- Influence employment and pay decisions

In the context of automated worker surveillance and management it is particularly important that the following responsible practices are enforced:

- Automated worker surveillance and management systems are used only in environments with high levels of worker protections and decision-making power
- Robust and substantive mechanisms exist for worker agency in identifying needs for automated systems, selecting vendors and systems, and implementing them in the workplace
• Meaningful, comprehensible explanation of the automated system's function and operation is provided to workers overseeing it, using it, or affected by it

• Transparency is provided about what worker data is collected, how it will be used, and why; workers are able to opt out of data collection

• Non-discrimination by automated workplace systems is ensured

• Human recourse is available into automated decisions or recommendations offered, including transparent, human-decided grievance redress mechanisms

• Automated worker surveillance is never used to predict the lowest wage a given worker would accept1

For more detailed information on the above, please refer to PAI’s Guidelines for AI and Shared Prosperity, in particular, the Signals of Risks and Responsible Practices sections.

---

Guidelines for AI and Shared Prosperity
Tools for improving AI’s impact on jobs
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Reference</td>
<td>3</td>
</tr>
<tr>
<td>Signals of Opportunity and Risk</td>
<td>3</td>
</tr>
<tr>
<td>Responsible Practices for Organizations</td>
<td>4</td>
</tr>
<tr>
<td>Get Involved</td>
<td>5</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>6</td>
</tr>
<tr>
<td>Learn About the Guidelines</td>
<td>7</td>
</tr>
<tr>
<td>The Need for the Guidelines</td>
<td>7</td>
</tr>
<tr>
<td>Origin of the Guidelines</td>
<td>8</td>
</tr>
<tr>
<td>Design of the Guidelines</td>
<td>9</td>
</tr>
<tr>
<td>Key Principles for Using the Guidelines</td>
<td>11</td>
</tr>
<tr>
<td>Apply the Job Impact Assessment Tool</td>
<td>14</td>
</tr>
<tr>
<td>Instructions for Performing a Job Impact Assessment</td>
<td>14</td>
</tr>
<tr>
<td>Signals of Opportunity for Shared Prosperity</td>
<td>15</td>
</tr>
<tr>
<td>Signals of Risk to Shared Prosperity</td>
<td>21</td>
</tr>
<tr>
<td>Follow Our Stakeholder-Specific Recommendations</td>
<td>28</td>
</tr>
<tr>
<td>Responsible Practices for AI-Creating Organizations (RPC)</td>
<td>28</td>
</tr>
<tr>
<td>Responsible Practices for AI-Using Organizations (RPU)</td>
<td>34</td>
</tr>
<tr>
<td>Suggested Uses for Policymakers</td>
<td>41</td>
</tr>
<tr>
<td>Suggested Uses for Labor Organizations and Workers</td>
<td>42</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>43</td>
</tr>
<tr>
<td>AI and Shared Prosperity Initiative’s Steering Committee</td>
<td>44</td>
</tr>
<tr>
<td>Endorsements</td>
<td>45</td>
</tr>
<tr>
<td>Sources</td>
<td>48</td>
</tr>
</tbody>
</table>

Though this document reflects the inputs of many PAI Partners, it should not be read as representing the views of any particular organization or individual within the AI and Shared Prosperity Initiative’s Steering Committee or any specific PAI Partner.
Quick Reference

Signals of Opportunity and Risk

**Signals of Opportunity for Shared Prosperity**
An opportunity signal (OS) is present if an AI system may:

**OS1.** Generate significant, widely distributed benefits

**OS2.** Boost worker productivity
  - Caveat 1: Productivity boosts can deepen inequality
  - Caveat 2: Productivity boosts can displace workers
  - Caveat 3: Productivity boosts can significantly hamper job quality

**OS3.** Create new paid tasks for workers
  - Caveat 1: Someone’s unpaid tasks can be someone else’s full-time job
  - Caveat 2: New tasks often go unacknowledged and unpaid

**OS4.** Support an egalitarian labor market

**OS5.** Be appropriate for lower-income geographies

**OS6.** Broden access to the labor market

**OS7.** Boost revenue share of workers and society

**OS8.** Respond to needs expressed by impacted workers

**OS9.** Be co-developed with impacted workers

**OS10.** Improve job quality or satisfaction
  - Caveat 1: Systems can improve one aspect of job quality while harming another
  - Caveat 2: AI systems are sometimes deployed to redress job quality harms created by other AI systems

**Signals of Risk to Shared Prosperity**
A risk signal (RS) is present if an AI system may:

**RS1.** Eliminate a given job’s core tasks

**RS2.** Reallocate tasks to lower-paid or more precarious jobs

**RS3.** Reallocate tasks to higher- or lower-skilled jobs

**RS4.** Move jobs away from geographies with few opportunities

**RS5.** Increase market concentration and barriers to entry

**RS6.** Rely on poorly treated or compensated outsourced labor

**RS7.** Use training data collected without consent or compensation

**RS8.** Predict the lowest wages a worker will accept

**RS9.** Accelerate task completions without other changes

**RS10.** Reduce schedule predictability

**RS11.** Reduce workers’ break time

**RS12.** Increase overall difficulty of tasks

**RS13.** Enable detailed monitoring of workers

**RS14.** Reduce worker autonomy

**RS15.** Reduce mentorship or apprenticeship opportunities

**RS16.** Reduce worker satisfaction

**RS17.** Influence employment and pay decisions

**RS18.** Operate in discriminatory ways
Responsible Practices for Organizations

Responsible Practices for AI-Creating Organizations (RPC)

RPC1. Make a public commitment to identify, disclose, and mitigate the risks of severe labor market impacts presented by AI systems you develop
RPC2. In collaboration with affected workers, perform Job Impact Assessments early and often throughout the AI system lifecycle
RPC3. In collaboration with affected workers, develop mitigation strategies for identified risks
RPC4. Source data enrichment labor responsibly
RPC5. Create and use robust and substantive mechanisms for worker participation in AI system origination, design, and development
RPC6. Build AI systems that align with worker needs and preferences
RPC7. Build AI systems that complement workers (especially those in lower-wage jobs), not ones that act as their substitutes
RPC8. Ensure workplace AI systems are not discriminatory
RPC9. Provide meaningful, comprehensible explanations of the AI system’s function and operation to workers using or affected by it
RPC10. Ensure transparency about what worker data is collected, how and why it will be used, and enable opt-out functionality
RPC11. Embed human recourse into decisions or recommendations you offer
RPC12. Apply additional mitigation strategies to sales and use in environments with low worker protection and decision-making power
RPC13. Red team AI systems for potential misuse or abuse
RPC14. Ensure AI systems do not preclude the sharing of productivity gains with workers
RPC15. Request deployers to commit to following PAI’s Shared Prosperity Guidelines or similar recommendations

Responsible Practices for AI-Using Organizations (RPU)

RPU1. Make a public commitment to identify, disclose, and mitigate the risks of severe labor market impacts presented by AI systems you use
RPU2. Commit to neutrality towards worker organizing and unionization
RPU3. In collaboration with affected communities, perform Job Impact Assessments early and often throughout AI system implementation and use
RPU4. In collaboration with affected communities, develop mitigation strategies for identified risks
RPU5. Create and use robust and substantive mechanisms for worker agency in identifying needs, selecting AI vendors and systems, and implementing them in the workplace
RPU6. Ensure AI systems are used in environments with high levels of worker protections and decision-making power
RPU7. Source data enrichment labor responsibly
RPU8. Ensure workplace AI systems are not discriminatory
RPU9. Procure AI systems that align with worker needs and preferences
RPU10. Staff and train sufficient internal or contracted expertise to properly vet AI systems and ensure responsible implementation
RPU11. Prefer vendors who commit to following PAI’s Shared Prosperity Guidelines or similar recommendations
RPU12. Ensure transparency about what worker data is collected, how it will be used, and why, and enable workers to opt out
RPU13. Provide meaningful, comprehensible explanations of the AI system’s function and operation to workers overseeing it, using it, or affected by it
RPU14. Establish human recourse into decisions or recommendations offered, including the creation of transparent, human-decided grievance redress mechanisms
RPU15. Red team AI systems for potential misuse or abuse
RPU16. Recognize extra work created by AI system use and ensure work is acknowledged and compensated
RPU17. Ensure mechanisms are in place to share productivity gains with workers
Get Involved

The Partnership on AI seeks to engage all interested stakeholders to refine, test, and drive the adoption and evolution of all parts of the Shared Prosperity Guidelines, including the Job Impact Assessment Tool, the Responsible Practices, and Suggested Uses. We also seek to curate a library of learnings, use cases and examples, as well as partner with stakeholders to co-create companion resources to help make the Guidelines easier to use for their communities.

We will pursue these goals by means of stakeholder outreach, dedicated workshops, and limited implementation collaborations. If you’re interested in engaging with us on this work or want to publicly endorse the Guidelines, please get in touch.
Executive Summary

Our economic future is too important to leave to chance.

AI has the potential to radically disrupt people’s economic lives in both positive and negative ways. It remains to be determined which of these we’ll see more of. In the best scenario, AI could widely enrich humanity, equitably equipping people with the time, resources, and tools to pursue the goals that matter most to them.

Our current moment serves as a profound opportunity — one that we will miss if we don’t act now. To achieve a better future with AI, we must put in the work today. Many societal factors outside the direct control of AI-developing and AI-using organizations will play a role in determining this outcome. However, much still depends on the choices those organizations make, as well as on the actions taken by labor organizations and policymakers.

You can help guide AI’s impact on jobs

AI-creating companies, AI-using organizations, policymakers, labor organizations, and workers can all help steer AI so its economic benefits are shared by all. Using Partnership on AI’s (PAI) Guidelines for AI & Shared Prosperity, these stakeholders can guide AI development and use towards better outcomes for workers and labor markets.

Included in the Guidelines are:

- a high-level Job Impact Assessment Tool for analyzing an AI system's positive and negative impact on shared prosperity
- a collection of Stakeholder-Specific Recommendations to help minimize the risks and maximize the opportunities to advance shared prosperity with AI

How to use the Guidelines

The Shared Prosperity Guidelines can be used by following a guided, three-step process.

Step 1
Learn about the Guidelines

Step 2
Apply the Job Impact Assessment Tool

Step 3
Follow our Stakeholder-Specific Recommendations
The Need for the Guidelines

Action is needed to guide AI's impact on jobs

Artificial intelligence is poised to substantially affect the labor market and the nature of work around the globe.

- Some job categories will shrink or disappear entirely and new types of occupations will arise in their place
- Wages will be affected, with AI changing the demand for various skills and the access workers have to jobs
- The tasks workers perform at their jobs will change, with some of their previous work automated and other tasks assisted by new technologies
- Job satisfaction and job quality will shift. Benefits will accrue to the workers with the highest control over how AI shows up in their jobs. Harms will occur for workers with minimal agency over workplace AI deployments

The magnitude and distribution of these effects is not fixed or pre-ordained. Today, we have a profound opportunity to ensure that AI's effects on the labor market and the future of work contribute to broadly shared prosperity.

In the best scenario, humanity could use AI to unlock opportunities to mitigate climate change, make medical treatments more affordable and effective, and usher in a new era of improved living standards and prosperity around the world. This outcome, however, will not be realized by default. It requires a concerted effort to bring it about. AI use poses numerous large-scale economic risks that are likely to materialize given our current path, including:

- Consolidating wealth in the hands of a select few companies and countries
- Reducing wages and undermining worker agency as larger numbers of workers compete for deskillled, lower-wage jobs
- Allocating the most fulfilling tasks in some jobs to algorithms, leaving humans with the remaining drudgery
- Highly disruptive spikes in unemployment or underemployment as workers start at the bottom rung in new fields, even if permanent mass unemployment does not arise in the medium term

Artificial intelligence is poised to substantially affect the labor market and the nature of work around the globe.

Example explanations of why technological change is the result of market-shaping policies (and not some "natural" or predetermined trajectory) can be found in:

Redesigning AI: Work, democracy, and justice in the age of automation

Steering technological progress

We use the definition of underemployment from Merriam-Webster dictionary: "the condition in which people in a labor force are employed at less than full-time or regular jobs or at jobs inadequate with respect to their training or economic needs."
The Guidelines are tools for creating a better future

Partnership on AI's (PAI) Shared Prosperity Guidelines are intended to equip interested stakeholders with the conceptual tools they need to steer AI in service of shared prosperity.

All stakeholders looking to ground their decisions, agendas, and interactions with each other in a systematic understanding of labor market opportunities and risks presented by AI systems can use these tools. This includes:

- AI-creating organizations
- AI-using organizations
- Policymakers
- Labor organizations and workers

Origin of the Guidelines

This work comes from years of applied research and multidisciplinary input

A key output of PAI’s AI and Shared Prosperity Initiative, PAI’s Shared Prosperity Guidelines were developed under the close guidance of a multidisciplinary Steering Committee and draw on insights gained during two years of applied research work. This work included economic modeling of AI’s impacts on labor demand, engaging frontline workers around the world to understand AI’s impact on job quality, mapping the levers for governing AI’s economic trajectory, as well as a major workstream on creating and testing practitioner resources for the responsible sourcing of data enrichment labor. The plan for this multi-stakeholder applied research work was shared with the public in “Redesigning AI for Shared Prosperity: an Agenda” published by Partnership on AI in 2021, following eight months of Steering Committee deliberations.

Though this document reflects the inputs of many PAI Partners, it should not be read as representing the views of any particular organization or individual within the AI and Shared Prosperity Initiative’s Steering Committee or any specific PAI Partner.
Design of the Guidelines

We offer two tools for guiding AI’s impact on jobs

A high-level Job Impact Assessment Tool with:

- Signals of Opportunity indicating an AI system may support shared prosperity
- Signals of Risk indicating an AI system may harm shared prosperity

A collection of Stakeholder-Specific Recommendations: Responsible Practices and Suggested Uses for stakeholders able to help minimize the risks and maximize the opportunities to advance shared prosperity with AI. In particular, they are written for:

- AI-creating organizations
- AI-using organizations
- Policymakers
- Labor organizations and workers

These tools can guide choices about any AI system

PAI's Shared Prosperity Guidelines are designed to apply to all AI systems, regardless of:

- Industry (including manufacturing, retail/services, office work, and warehousing and logistics)
- AI technology (including generative AI, autonomous robotics, etc.)
- Use case (including decision-making or assistance, task completion, training, and supervision)

As a whole, the Guidelines are general purpose and applicable across all existing AI technologies and uses, though some sections may only apply to specific technologies or uses.

To apply these guidelines, stakeholders should:

- For an AI system of interest, perform the analysis suggested in the Job Impact Assessment section, identifying which signals of opportunity and risk to shared prosperity are present.
- Use the results of the Job Impact Assessment to inform your plans, choices, and actions related to the AI system in question, following our Stakeholder-Specific Recommendations. For AI-creating and AI-using organizations, these recommendations are Responsible Practices. For policymakers, unions, workers, and their advocates, these recommendations are Suggested Uses.

We look forward to testing the Guidelines and refining the use scenarios together with interested stakeholders. If you have suggestions or would like to contribute to this work, please get in touch.
Our approach focuses on AI’s impact on labor demand

In these Guidelines, we consider an AI system to be serving to advance the prosperity of a given group if it boosts the demand for labor of that group — since selling labor remains the primary source of income for the majority of people in the world.

We recognize that some communities advocate to advance shared prosperity in the age of AI through benefits redistribution mechanisms such as universal basic income. While a global benefits redistribution mechanism might be an important part of the solution (especially in the longer term) and we welcome research efforts and public debate on this topic, we left it outside of the scope of the current version of the Guidelines.

Instead, the Guidelines focus on governing the impact of AI on labor demand. We believe this approach will be extremely necessary at least in the short to medium term, enabling communities to have effective levers of influence over the pace, depth, and distribution of AI impacts on labor demand.

AI’s impacts on labor demand can manifest themselves as:

- Changes in availability of jobs for certain skill, demographic, or geographic groups
- Changes in the quality of jobs affecting workers’ well-being

In line with PAI’s framework for promoting workforce well-being in the AI-integrated workplace and other leading resources on high-quality jobs, we recognize multiple dimensions of job quality or workers’ well-being, namely:

- Human rights
- Financial well-being
- Physical well-being
- Emotional well-being
- Intellectual well-being
- Sense of meaning, community, and purpose.

Thus, for the purposes of these Guidelines, we define AI’s impact on shared prosperity as the impact of AI use on availability and quality of formal sector jobs across skill, demographic, or geographic groups.

In turn, the overall impact of AI on the availability and quality of jobs can be anticipated as a sum total of changes in the primary factors AI use is known to affect. Those factors are:

---

C Groups’ boundaries can be defined geographically, demographically, by skill type, or another parameter of interest.

D In other words, AI’s impact on labor demand can affect both incumbent workers as well as people interested in looking for work in the present or future.

E The share of informal sector employment remains high in many low- and middle-income countries. The emphasis on formal sector jobs here should not be interpreted as treating the informal sector as out of scope of the concern of PAI’s Shared Prosperity Guidelines. The opposite is the case: if the introduction of an AI system in the economy results in a reduction of availability of formal sector jobs, that reduction cannot be considered to be compensated by growth in availability of jobs in the informal sector.
• Relative productivity of workers (versus machines or workers in other skill groups)
• Labor’s share of organization revenue
• Task composition of jobs
• Skill requirements of jobs
• Geographic distribution of the demand for labor
• Geographic distribution of the supply of labor
• Market concentration
• Job stability
• Stress rates
• Injury rates
• Schedule predictability
• Break time

• Job intensity
• Freedom to organize
• Privacy
• Fair and equitable treatment
• Social relationships
• Job autonomy
• Challenge level of tasks
• Satisfaction or pride in one’s work
• Ability to develop skills needed for one’s career
• Human involvement or recourse for managerial decisions (such as performance evaluation and promotion)
• Human involvement or recourse in employment decisions (such as hiring and termination)

Anticipated effects on the above primary factors are the main focus of the risks and opportunities analysis tool provided in the Guidelines. Another important focus is the distribution of those effects. An AI system may bring benefits to one set of users and harms to another. Take, for example, an AI system used by managers to set and monitor performance targets for their reports. This system could potentially increase pride in one’s work for managers and raise rates of injury and stress for their direct reports.

When this dynamic prompts conflicting interests, we suggest higher consideration for the more vulnerable group with the least decision-making power in the situation as these groups often bear the brunt of technological harms. By a similar logic, where we call for worker agency and participation, we suggest undertaking particular effort to include the workers most affected and/or with the least decision authority (for example, the frontline workers, not just their supervisors).

Key Principles for Using the Guidelines

These application principles apply independently of who is using the Guidelines and in what specific scenario they are doing so.

Engage affected workers

Make sure to engage worker communities that stand to be affected by the introduction of an AI system in the Job Impact Assessment, as well as in the development of risk mitigation strategies. This includes, but is not limited to, engaging and affording agency to workers who will be affected by the AI system and their representatives. Bringing in multi-disciplinary experts will help understand the full spectrum and severity of the potential impact.
Workers may work with AI systems or have their work affected by them. In cases where one group of workers uses an AI system (for instance, uses an AI performance evaluation tool to assess their direct reports) and another group is affected by that AI system's use (in this example, the direct reports), we suggest giving highest consideration to affected workers and/or the workers with the least decision-making power in the situation (in this example, the direct reports rather than the supervisors).

**Seeking shared prosperity doesn’t mean opposing profits**

Some of the signals of risk to shared prosperity described in the Guidelines are actively sought by companies as profit-making opportunities. The Guidelines do not suggest that companies should stop seeking profits, just that they should do so responsibly.

Profit-generating activities do not necessarily have to harm workers and communities, but some of them do. The presence of signals of risk indicate that an AI system being assessed, while possibly capable of generating profit for a narrow set of beneficiaries, is likely to do that at the expense of shared prosperity, and thus might be undesirable from the societal benefit perspective. We encourage companies to follow the Guidelines, developing and using AI in ways that generate profit while also advancing shared prosperity.

**Signals are indicators, not guarantees**

Presence of a signal should be interpreted as an early indicator, not a guarantee that shared prosperity will be advanced or harmed by a given AI system. Presence of opportunity or risk signals for an AI system being assessed is a necessary, but not sufficient, condition for shared prosperity to be advanced or harmed with the introduction of that AI system into the economy.

Many societal factors outside of the direct control of AI-creating organizations play a role in determining which opportunities or risks end up being realized. Holding all other societal factors constant, the purpose of these Guidelines is to minimize the chance that shared prosperity-relevant outcomes are worsened and maximize the chance that they are improved as a result of choices by AI-creating and -using organizations and the inherent qualities of their technology.

**Signals should be considered comprehensively**

Signals of opportunity and risk should be considered comprehensively. Presence of a signal of risk does not automatically mean an AI system in question should not be developed or deployed. That said, an absence of any signals of opportunity does mean that a given AI system is highly unlikely to advance shared prosperity and whatever risks it might be presenting to society are not justified.
Signals of opportunity do not “offset” signals of risk

Presence of signals of opportunity should not be interpreted as “offsetting” the presence of signals of risk. In recognition that benefits and harms are usually borne unevenly by different groups, the Guidelines strongly oppose the concept of a “net benefit” to shared prosperity, which is incompatible with a human rights-based approach. In alignment with the UN Guiding Principles on Business and Human Rights, a mitigation strategy should be developed for each risk identified, prioritizing the risks of the most severe impacts first. Mitigation strategies can range from eliminating the risk or reducing the severity of potential impact to ensuring access to remedy or compensation for affected groups. If effective mitigation strategies for a given risk are not available, it should be considered as a strong argument in favor of meaningful changes in the development, implementation, and use plans of an AI system, especially if it is expected to affect vulnerable groups.

Analysis of signals is not prescriptive

The analysis of signals of opportunity and risk is not prescriptive. Decisions around the development, implementation, and use of increasingly powerful AI systems should be made collectively, allowing for the participation of all affected stakeholders. We anticipate that two main uses of the signals analysis will include:

- Informing stakeholders’ positions in preparation for dialogue around development, deployment, and regulation of AI systems, as well as appropriate risk mitigation strategies
- Identifying key areas of potential impact of a given AI system which warrant deeper analysis (such as to illuminate their magnitude and distribution) and further action

PAI’s Shared Prosperity Guidelines use UNGP’s definition of severity: an impact (potential or actual) can be severe “by virtue of one or more of the following characteristics: its scale, scope or irremediability. Scale means the gravity of the impact on the human right(s). Scope means the number of individuals that are or could be affected. Irremediability means the ease or otherwise with which those impacted could be restored to their prior enjoyment of the right(s).”
STEP 2
Apply the Job Impact Assessment Tool

Use the high-level Job Impact Assessment Tool to analyze a given AI system:

- Go over the full list of signals of opportunity and risk
- Analyze the distribution of potential benefits and harms
- Repeat this process for upstream and downstream markets

Instructions for Performing a Job Impact Assessment

Assess the AI system against the full list of signals

Go over the full list of signals of opportunity and risk and document which signals are present in the case of the AI system being assessed. Not all signals apply for every AI system. Document those that do not apply as not applicable, but do not skip or cherry-pick signals. For each step, document the explanation for the answer for future reference.

For each signal, if you estimated the likelihood of the respective opportunity or risk materializing as a result of the introduction of the AI system into the economy to be anything but “zero,” please note the respective signal as “present.”

Certainty in likelihood estimation is not a prerequisite for this high-level assessment and is assumed to be absent in most cases. When in doubt, note the signal as “present.”

Analyze the distribution of potential benefits and harms

Document in as much detail as possible your understanding of the distribution of potential benefits and harms of an AI system across skill, geographic, and demographic groups, and how it might change over time.1 (Are today’s “winners” expected to lose their gains in the future? The reverse?) The exact steps needed to perform the distribution of impacts analysis are highly case-specific. PAI is looking to engage with stakeholders to curate a library of distribution analysis examples for the community to learn from. If you would like to contribute to this, please get in touch.

Repeat this process for upstream and downstream markets

In order to take into account the possible effects on the competitors, suppliers, and clients of the AI-using organization, repeat the signal detection and analysis processes not only
for the primary market the AI system is intended to be deployed in, but also upstream and downstream markets.

Proceed to our Stakeholder-Specific Recommendations

After completing the high-level Job Impact Assessment analysis, 
**AI-creating** and 
**AI-using organizations** should implement recommended Responsible Practices (where not already in use) to improve anticipated outcomes — for instance, to eliminate or mitigate anticipated harms or increase likely benefits for workers and the economy. These Responsible Practices can be found under Step 3 of the Shared Prosperity Guidelines. (Responsible Practices will be added and refined through community testing and feedback.)

**Policymakers, workers and their representatives** can use the results of the high-level Jobs Impact Assessment to inform their decisions, actions, and agendas as outlined in the Suggested Uses section under Step 3 of the Shared Prosperity Guidelines. We look forward to collecting feedback on the Guidelines and curating use examples in partnership with interested stakeholders. To get involved, please **get in touch**.

⚠️ **Signals of Opportunity for Shared Prosperity**

If one or more of the statements below apply to the AI system being assessed, this indicates a possibility of a positive impact on shared prosperity-relevant outcomes.

**An opportunity signal (OS) is present if an AI system may:**

(OS1. Generate significant, widely distributed benefits)

Will the AI system generate significant, widely distributed benefits to the planet, the public, or individual consumers? One of the primary motivations for investing in the research and development of AI is its potential to help humanity overcome some of our most pressing challenges, including ones related to climate change and the treatment of disease. Hence, the potential of an AI system to generate public goods or benefit the environment is a strong signal of opportunity to advance shared prosperity.

Individual consumer benefits can be more controversial as many advocates point out the growing environmental costs that frequently accompany the commodification of consumer goods. But if production and consumption are environmentally conscious, a potential to generate significant and widely distributed consumer benefits is a signal of opportunity to advance shared prosperity. Cheaper or more high-quality goods or services make consumers richer in real terms, freeing up parts of their incomes to be spent to buy other goods and services, boosting the demand for labor in respective sectors of the economy.

How significant and widely distributed consumer benefits should be to justify job losses...
is a political question; but quantifying consumer gains per job lost would help sharpen up any debate about the value of an AI innovation. As stated in “Key Principles for Using the Guidelines,” independently of the magnitude and distribution of anticipated benefits, appropriate mitigation strategies should be developed in response to the risk of job losses or wage decreases.

**OS2. Boost worker productivity**

Will the AI system boost productivity of workers, in particular those in lower-paid jobs, without increasing strain? By a worker’s productivity, we mean a worker’s output per hour. A more productive worker is more valuable to their employer and (all other conditions remaining the same) is expected to be paid more. Therefore, if an AI system comes with a promise of a productivity boost that is a positive signal. Besides, productivity growth is often the prerequisite for the creation of consumer benefits discussed in OS1.

However, three important caveats should be noted here.

**Caveat 1: Productivity boosts can deepen inequality**

It is quite rare for a technology to equally boost productivity for everyone involved in the production of a certain good, more often it helps workers in certain skill groups more than others. If it is helping workers in lower-paying jobs relatively more, the effect could be inequality-reducing. Otherwise, it may be inequality-deepening. Please document the distribution of the productivity increase across the labor force when assessing the presence of this opportunity signal.

**Caveat 2: Productivity boosts can displace workers**

Even if productivity of all workers involved in the production of a certain good is boosted equally by an AI system, fewer of them might find themselves employed in the production of that good once the AI system is in place. This is because fewer (newly more productive) worker-hours are now needed to create the same volume of output. For production of the good in question to require more human labor after AI deployment, **two conditions must be met:**

- Productivity gains of the firm introducing AI need to be shared with its clients (such as consumers, businesses, or governments) in the form of lower-priced or higher-quality products — something which is less likely to happen in a monopolistic environment
- Clients should be willing to buy sufficiently more of that lower-priced or higher-quality product

If the first condition is met but the second is not, the introduction of the AI system in question might still be, on balance, labor-demand boosting if it induces a “productivity effect” in the broader economy. When productivity gains and corresponding consumer benefits are sufficiently large, consumers will experience a real income boost generating new labor demand in the production of complementary goods. That new labor demand might be sufficient to compensate for the original loss of employment due to an introduction of an AI system. Issues arise when the productivity gains are too small like in the case of “so-so” technologies or are not shared with consumers. If that is the case, please document OS2 as “not present” when performing the Job Impact Assessment.

---

**L** For example, in 2011, the US government imposed tariffs to prevent job losses in the tire industry. Economic analysis later showed that the tariffs cost American consumers around $0.9 million per job saved. It seems implausible that such large consumer costs are worthwhile, relative to the job gains.

**M** In this paper, Brynjolfsson et al. estimate the value of many free digital goods and services. They do so by proposing a new metric called GDP-B, which quantifies their benefits rather than costs, and then estimating consumers’ willingness-to-pay for free digital goods and services in terms of GDP-B.

**N** As emphasized in Key Principles for Using the Guidelines, signals of opportunity are not guarantees: it is possible that the introduction of a new technology into the workplace boosts workers' productivity but does not lead to wage growth because, in practice, workers’ productivity is only one of the factors determining their wage. Other factors include how competitive the market is and how much bargaining power workers have. In fact, a large number of countries have been experiencing productivity-wage decoupling in recent decades. This points to a diminishing role of productivity in determining wages, but it remains non-zero and hence has to be accounted for by the Guidelines.

**O** The impact of a productivity-enhancing technology can manifest itself as a reduction of the size of the workforce, or a reduction in hours worked by the same-size labor force. Either option can negatively impact shared prosperity.
Caveat 3: Productivity boosts can significantly hamper job quality
Introduction of an AI system can lead to productivity enhancement through various routes: by allowing workers to produce more output per hour of work at the same level of effort or by allowing management to induce a higher level of effort from workers. If productivity boosts are expected to be achieved solely or mainly through increasing work intensity, please document OS2 as “not present” when performing the Job Impact Assessment.

Lastly, frontline workers reported appreciation for AI systems that boosted their productivity by assisting them with core tasks. Conversely, technologies that boosted productivity by automating workers’ core tasks were associated with a reduction in job satisfaction. Hence, pursuit of productivity increases through technologies that eliminate non-core tasks is preferred over paths that involve eliminating core tasks. Examples of technologies that assist workers on their core tasks include:

- Training and coaching tools
- Algorithmic decision support systems that give users additional information, analytics, or recommendations without prescribing or requiring decisions

**OS3. Create new paid tasks for workers**

Will the AI system create new tasks for humans or move unpaid tasks into paid work?

Technological innovations have a great potential for benefit when they create new formal sector jobs, tasks, or markets that did not exist before. Consider, for example, the rise of social media influencers and content creators. These types of jobs were not possible before the rise of contemporary media and recommendation technologies. It has been estimated that, in 2018, more than 60 percent of employees were employed in occupations that did not exist in 1940.

**Caveat 1: Someone’s unpaid tasks can be someone else’s full-time job**

It is important to keep in mind that technologies seemingly moving unpaid tasks into paid ones might, upon closer inspection, be producing an unintended (or deliberately unadvertised) effect of shifting tasks between paid jobs — often accompanied by a job quality downgrade. For example, a technology that allows people to hire someone to do their grocery shopping might convert their unpaid task into someone else’s paid one, but also reduce the demand for full-time domestic help workers, increasing precarity in the labor market.

**Caveat 2: New tasks often go unacknowledged and unpaid**

Sometimes the introduction of an AI system adds unacknowledged and uncompensated tasks to the scope of workers. For example, the labor of smoothing the effects of machine malfunction remains under the radar in many contexts, creating significant unacknowledged burdens on workers who end up responsible for correcting machine’s errors (without being adequately positioned to do that).

When performing the Job Impact Assessment, please explicitly document the applicability of these two caveats associated with OS3 for the AI system being assessed and its deployment context.

**OS4. Support an egalitarian labor market**

Will the AI system support a more egalitarian labor market structure? A superstar labor market structure is a situation where a relatively small number of workers dominate the market or satisfy most of the labor demand that exists in it. The opposite is an “egalitarian” labor structure where each worker’s output is small relative to the output of all other...
workers in the industry. The key factor that makes a labor market's structure egalitarian is the presence of a need to invest an additional unit of worker time to serve an additional consumer. For example, the rise of the music recording industry has made its labor market structure less egalitarian for musicians. Today, to satisfy the demand for music from an additional customer, musicians do not need to physically get in front of them or do any additional work.

**OS5. Be appropriate for lower-income geographies**

Will the AI system be appropriate for lower-income geographies? Capital and labor of various skill types can be relatively more or less abundant in different countries. Technologies that take advantage of the factor of production (capital or labor of a certain skill type) that is relatively more abundant in a given country and do not require much of a factor that is relatively scarce are deemed appropriate for that country.

Generally, capital is relatively more abundant in the higher-income countries while labor is relatively more abundant in the lower-income countries, many of which also struggle with poor learning outcomes limiting the training the workforce receives. Therefore, capital-intensive labor-saving AI systems are generally inappropriate for lower-income countries whose main comparative advantage is relatively abundant labor. Such technologies being adopted by high-income countries can hurt economic outcomes in lower-income countries because competitive forces in the export industries force the latter to adopt those technologies to remain competitive.

Consequently, lower-income countries would greatly benefit from access to technologies that would allow them to stay competitive by leveraging their abundant labor resources and creating gainful jobs that do not require high levels of educational attainment.

When assessing the presence of this signal, please also document if and how the relative abundance of capital and labor of various skill types is expected to change over time.

**OS6. Broaden access to the labor market**

Will the AI system broaden access to the labor market? AI systems that allow communities with limited or no access to formal employment to get access to gainful formal sector jobs are highly desirable from the perspective of broadly shared prosperity. Examples include AI systems that:

- Assist the disabled
- Make it easier to combine work and caregiving responsibilities
- Enable work in languages the worker does not have a fluent command of

**OS7. Boost revenue share of workers and society**

Will the AI system boost workers’ and society’s share of an organization’s revenue?
Workers' share of revenue is the percentage of an organization's revenue spent on workers' wages and benefits. For the purposes of these Guidelines, we suggest excluding C-suite compensation when calculating workers' share.

If, following the introduction of an AI system, workers' share of organization's revenue is expected to grow or at least stay constant, it is a very strong signal that the AI system in question will serve to advance shared prosperity. The opposite is also true. If, following the introduction of an AI system, workers' share of organization's revenue is expected to shrink, it is a very strong signal that the AI system in question will harm shared prosperity.

Please note that worker benefits are included in workers' share of an organization's revenue. For example, consider an organization that adopts a productivity-enhancing AI system which allows it to produce the same or greater amount of output with fewer hours of work needed from human workers. That organization can decide to retain the same size of the workforce and share productivity gains with it (for example, in the form of higher wages, longer paid time off, or shorter work week at constant weekly pay), keeping the workers' share of revenue constant or growing. That would be a prime example of using AI to advance shared prosperity.

Lastly, if an organization was able to generate windfall gains from AI development or usage and is committed to sharing the gains not only with workers it directly employs but the rest of the world's population as well, that can be a great example of using AI to advance shared prosperity. While some have proposed this, more research is needed to design mechanisms for making sure windfall gains are distributed equitably and organizations can be expected to reliably honor their commitment to distribute their gains.

**OS8. Respond to needs expressed by impacted workers**

Did workers who will use the AI system or be affected by it (or their representatives) identify the need for the system? AI systems created from a worker's idea or identified need build in workers' job expertise and preferences from the outset, making it more likely the AI systems will be beneficial or useful to workers affected by them and welcomed as such. Much of the current AI development pipeline starts with advances in research and development, only later identifying potential applications and product-market fit. The market for workplace AI technology is largely composed of senior executives and managers, creating a potential misalignment between needs perceived by budget holders and managers and the needs perceived by the workers who use or are most affected by the technology. AI systems emerging from the ideas and needs of workers who use or are most affected by them (or their representatives, who represent the collective voice of a given set of workers, not just the perspective of an individual worker) reduce this potential for misalignment.
**OS9. Be co-developed with impacted workers**

Were workers who will ultimately use or be affected by the AI system (or their representatives) included and given agency in every stage of the system's development? Workers are subject matter experts in their own tasks and roles, and can illuminate opportunities and challenges for new technologies that are unlikely to be seen by those with less familiarity with the specifics of the work. The wisdom of workers who use or are most affected by AI systems introduced throughout development can smooth many rough edges that other contributors might only discover after systems are in the market and implemented. Where relevant worker representatives exist, they should be brought into the development process to represent collective worker interests from start to finish.

Fully offering affected workers agency in the development process requires taking the time to understand their vantage points, and equip them or their representatives with enough knowledge about the proposed technology to meaningfully participate. They also must be afforded sufficient decision-making power to steer projects and, if necessary, end them in instances where unacceptable harms cannot be removed or mitigated. This also necessitates protecting their ability to offer suggestions freely without fear of repercussions. Without taking these steps, participatory processes can still lead to suboptimal outcomes — and possibly create additional harms through covering problems with a veneer of worker credibility.

**OS10. Improve job quality or satisfaction**

Was the AI system intended to improve job quality or increase job satisfaction? AI technology has the potential to improve many aspects of job quality and job satisfaction, from increasing occupational safety to providing personalized coaching that leads to career advancement. This requires taking job quality, worker needs, and worker satisfaction seriously.

Two important caveats are required for this signal.

Caveat 1: Systems can improve one aspect of job quality while harming another
For example, many AI technologies positioned as safety enhancements are in reality invasive surveillance technologies. Though safety improvements may occur, harms to human rights, stress rates, privacy, job autonomy, job intensity, and other aspects of job quality may occur as well. Other AI systems purport to improve job quality by automating tasks workers dislike (see RS1 for more detail on the risks of task elimination).

When a system enhances one aspect of job quality while endangering another, this signal can still be counted as “present,” but the need to consider the rest of the opportunity and risk signals is particularly important.

Caveat 2: AI systems are sometimes deployed to redress job quality harms created by other AI systems
For example, some companies have introduced AI safety technologies to correct harms resulting from the prior introduction of an AI performance target-setting system that encouraged dangerous overwork.25
When this is the case, the introduction of the new AI system to redress the harms of the old does not count for this signal and should be marked as “not present.”

Instead of introducing new AI systems with their own attendant risks, the harms from the existing systems should be addressed in line with the Responsible Practices provided by the Guidelines for AI-using organizations and additional case-specific mitigations.

⚠️ Signals of Risk to Shared Prosperity

If one or more of the statements below apply to the AI system being assessed, this indicates a possibility of a negative impact on shared prosperity–relevant outcomes.

Some of the signals of risk to shared prosperity described in the Guidelines are actively sought by companies as profit-making opportunities. The Guidelines DO NOT suggest that companies should stop seeking profits, just that they should do so responsibly.

Profit-generating activities do not necessarily have to harm workers and communities, but some of them do. The presence of signals of risk indicate that an AI system being assessed, while possibly capable of generating profit for a narrow set of beneficiaries, is likely to do that at the expense of shared prosperity, and thus might be undesirable from the societal benefit perspective. We encourage companies to follow the Guidelines, developing and using AI in ways that generate profit while also advancing shared prosperity.

For-profit companies might feel pressure from investors to cut their labor costs no matter the societal price. We encourage investors and governments to join civil society in an effort to incentivize responsible business behavior with regards to shared prosperity and labor market impact.

Some practices or outcomes included in this section are illegal in some jurisdictions, and as such are already addressed in those locations. We include them here due to their legality in other jurisdictions.

A risk signal (RS) is present if an AI system may:

RS1. Eliminate a given job’s core tasks

Will the AI system eliminate a significant share of tasks for a given job? A lot of technological innovations eliminate some job tasks that were previously done by human workers. That is not necessarily an unwelcome development, especially when those technologies also create new paid tasks for humans (see OS3), boost job quality (see OS10), or bring significant broadly distributed benefits (see OS1). For example, it can be highly desirable to automate tasks posing unmitigable risks to workers’ physical or mental health. Primary research conducted by the AI and Shared Prosperity Initiative indicated that frontline workers often experience automation of their non-core tasks as helpful and productivity-boosting.29
However, if an AI system is primarily geared towards eliminating core paid tasks without much being expected in terms of increased job quality or broadly shared benefits, nor in terms of new tasks for humans being created in parallel, then it warrants further attention as posing a risk to shared prosperity. The introduction of such a system will likely lower the demand for human labor, and thus wage or employment levels for affected workers. Automation of core tasks can also be experienced by workers as directly undermining their job satisfaction since workers’ core responsibilities are closely tied to their sense of pride and accomplishment in their jobs. For workers who see their jobs as an important part of their identity, core tasks are a major aspect of how they see themselves in the world. Automation of core tasks can also lower the skill requirements of a job and reduce the formation of skills needed to advance to the next level.

Please note that to evaluate the share of a given job’s tasks being eliminated, those tasks should be weighted by their importance for the production of the final output. We consider task elimination above 10% significant enough to warrant attention.

**RS2. Reallocate tasks to lower-paid or more precarious jobs**

Will the AI system enable reallocation of tasks to lower-paid or more precarious jobs or informal or unpaid labor? Often, while not eliminating human tasks on balance, AI technology enables shifting tasks from full-time jobs to unpaid or more precarious labor. The latter can happen, for example, through the “gig-ification” of work: technologically enabled separation of “time on task” and “idle time” which leads to unstable and unpredictable wages as well as the circumvention of minimum wage laws.

Paid tasks can also be converted into unpaid when new technology enables them to be performed by customers. Examples of that are self-checkout kiosks or automated customer support.

**RS3. Reallocate tasks to higher- or lower-skilled jobs**

Will the AI system enable the reallocation of tasks to jobs with higher or lower specialized skills requirements? Jobs with higher specialized skills requirements generally are better compensated, hence an AI system shifting tasks into such jobs will likely lead to a positive effect of more of them being opened up. However, those jobs might not be accessible to people affected by task reallocation because those people might not possess the newly required specialized skills. Retraining and job matching support programs can help here, though those often fall short. Word processor is an example of a technology that reallocated typing-related tasks away from typists to managers. Generative AI applications are an example of a recent technology anticipated to induce broad-reaching shifts in skill requirements of large swaths of jobs.

Importantly, AI-induced reallocation of tasks to jobs with lower specialized skills requirements may be positive but is still a risk signal warranting further attention, because...
lowering specialized skill requirements can lower not only the barriers to entry to the occupation, but also prevailing wages.

**RS4. Move jobs away from geographies with few opportunities**

Will the AI system move job opportunities away from geographies where there would be few remaining? Due to associated costs and excessive immigration barriers, labor mobility remains low, both within and between countries. As a result, changes that move job opportunities from one area to another can harm workers in the losing area. Research suggests that disappearance of stable, well-paying jobs can profoundly re-shape regions, leading to a rise in “deaths of despair,” addictions, and mental health problems.\(^{35}\)\(^{36}\) Impacted communities might be able to bounce back from job loss if comparable alternative job opportunities are sufficiently available in their area. But even when those exist, the presence of labor market frictions make it important to invest in creating support programs to help workers move into new jobs of comparable quality.

In addition to jobs disappearing as the direct effect of labor-saving technology being introduced in a region, please note that this effect can also be an indirect result of labor-saving technology initially introduced in a completely different region or country. Due to excessive immigration barriers, AI developers based in high-income countries face massively inflated incentives to create labor-saving technologies far in excess of what would be socially optimal given the world’s overall level of labor supply/demand for jobs.\(^{37}\)

Once that technology is developed in the high-income countries it gets deployed all over the world, including countries facing a dire need of formal sector jobs.\(^{38}\)

**RS5. Increase market concentration and barriers to entry**

Will an AI system increase market concentration and barriers to market entry? An increase in market concentration is a signal of a possible labor market impact to come for at least two reasons:

- It increases the risk of job cuts by competing firms
- It makes it less likely that the winning firm shares efficiency gains with workers in the form of better wages/benefits or with consumers in the form of lower prices/higher-quality products

Therefore, in a monopolistic market, any benefits brought on by AI are likely to be shared by few, while the harms might still be widely distributed. Similarly, job impacts that might occur in upstream or downstream industries due to an AI-induced increase in market concentration need to be accounted for as well.

**RS6. Rely on poorly treated or compensated outsourced labor**

Will the AI system rely on, for either model training or operation, outsourced labor deprived of a living wage and decent working conditions? The process of building datasets for
model training can be highly labor-intensive. It often requires human workers (whom we will refer to as data enrichment professionals) to review, classify, annotate, and otherwise manage massive amounts of data. Despite the foundational role played by data enrichment professionals, a growing body of research reveals the precarious working conditions that they face, which include:

- Inconsistent and unpredictable compensation for their work
- Unfairly rejected and therefore unpaid labeling tasks
- Long, ad-hoc working hours
- Lack of means to contest or get an explanation for the decisions affecting their take-home pay and ratings
- Lack of transparency around data enrichment labor sourcing practices in the AI industry exacerbate this issue.

**RS7. Use training data collected without consent or compensation**

Will the AI system be trained using a dataset containing data collected without consent and/or compensation? AI systems can be trained on data that embeds the economically-relevant know-how of people who generated that data, which can be especially problematic if the subsequent deployment of that AI system reduces the demand for labor of those people. Examples include but are not limited to:

- Images created by artists and photographers that are used to train generative AI systems
- Keystrokes and audio recordings of human customer service agents used to create automated customer service routines
- Records of actions taken by human drivers used to train autonomous driving systems

**RS8. Predict the lowest wages a worker will accept**

Will the AI system be used to predict the lowest wage a given worker would accept? It has been documented that workers can experience the impact of AI systems used for workforce management as effectively depriving them of being able to predict their take-home wages with any amount of certainty. An AI system allowing predictions about the lowest wages an individual worker would accept is analogous to a system allowing for perfect price discrimination of consumers. Price discrimination, while always driven by monopoly power and thus inefficient, is considered acceptable in certain situations, such as reduced price of museum admission for seniors and students. However, that acceptability is predicated on the transparency of the underlying logic. A possibility of using an algorithmic system to create take-home pay “personalization,” especially based on logic that is opaque to the workers or ever-changing, should serve as a strong signal of a potential negative impact on shared prosperity. A related risk for informal workers is the use of AI to reduce their bargaining power relative to those they contract with. Information asymmetries created through AI use by purchasers of their work are an emerging risk to workers in the informal sector.
RS9. Accelerate task completions without other changes

Will the AI system accelerate task completion without meaningfully changing resources, tools, or skills needed to accomplish the tasks? Some AI systems push workers to higher performance on goals, targets, or KPIs without modifying how the work is done. Examples of this include speeding up the pace with which workers are expected to complete tasks or using AI to set performance goals that are just out of reach for many workers. When this occurs without additional support for workers in the form of streamlining, simplifying, or otherwise improving the process of completing the task, it risks higher stress and injury rates for workers.

RS10. Reduce schedule predictability

Will the AI system reduce the amount of advance notice a worker receives regarding changes to their working hours? Schedule predictability is strongly tied to workers' physical and mental health. Automated, last-minute scheduling software can harm workers:

- Emotional well-being through increased stress
- Occupational safety and health through sleep deprivation/unpredictability and the physical effects of stress
- Financial well-being through missed shifts and increased need for more expensive transit (for example, ride-hailing services at times when public transit isn't frequent or safe).

Recent AI technology designed to lower labor costs by reducing the number of people working during predicted “slow” times has disrupted schedule predictability, with workers receiving minimal notice about hours that have been eliminated from or added to their schedules.

RS11. Reduce workers' break time

Will the AI system infringe on workers' breaks or encourage them to do so? Workers' breaks are necessary for their recovery from physically, emotionally, or intellectually strenuous or intense periods of work, and are often protected by law. Some AI systems billed as productivity software infringe on workers' breaks by sending them warnings based on the time they've spent away from their workstations or “off-task,” even during designated breaks or while they are using allotted break time. Others implicitly encourage workers to skip breaks by setting overly ambitious performance targets that pressure workers to work through downtime to meet goals. These systems can foster higher rates of injury or stress, undermine focus, and reduce opportunities to form social relationships at work.

RS12. Increase overall difficulty of tasks

Will the AI system increase the overall difficulty of tasks? When AI systems are used to automate less demanding tasks (for example, the most straightforward, emotionally
neutral customer requests in a call center), workers may be left with a higher concentration of more demanding tasks, effectively increasing the difficulty of their job. Difficulty increases may take the form of more physically, emotionally, or intellectually demanding tasks. The higher intensity may also place them at higher risk of burning out. While some workers may welcome the added challenge, the above concerns merit caution, especially if workers are not compensated equitably for the increased difficulty.

**RS13. Enable detailed monitoring of workers**

Will the AI system monitor something other than the pace and quality of task completion? The use of AI to monitor workers is just the latest entry in the long history of the technological surveillance of labor. However, AI capabilities have increased the frequency, comprehensiveness, and intensiveness of on-the-job monitoring. This use of AI often extends beyond monitoring of workers’ direct responsibilities and outputs, including information as varied as their time in front of their computer or time spent actively using their computer, their movements through an in-person worksite, and the frequency and content of communications with other workers. This detailed monitoring risks:

- Increasing stress and anxiety
- Harming their privacy
- Causing them to feel a lack of trust from their employer
- Undermining their sense of autonomy on the job
- Lowering engagement and job satisfaction
- Chilling worker organizing, undermining worker voice.

While monitoring systems can have legitimate uses (such as enhancing worker safety), even good systems can be abused, particularly in environments with low worker agency or an absence of regulations, monitoring, and enforcement of worker protections.

**RS14. Reduce worker autonomy**

Will the AI system reduce workers’ autonomy, decision-making authority, or control over how they complete their work? Autonomy, decision-making authority, job control, and the exercise of discernment in performing one’s job are correlated with high job quality and job satisfaction. Reducing scope for these activities could also be a sign of a shift from a “high-road” staffing approach (where experience and expertise is valued) to a “low-road” approach (where less training or experience is needed and thus workers hold less bargaining power and can be more easily replaced). In the informal sector, this may appear as a reduction in the scope for design and creativity by artisans and garment workers.

**RS15. Reduce mentorship or apprenticeship opportunities**

Will the AI system reduce workers’ opportunities for mentorship or apprenticeship? Automated training, automated coaching, and automation of entry-level tasks may
lower workers’ opportunities for apprenticeship and mentorship. Apprenticeship is an important way for workers to learn on the job, and develop the skills they need to advance. Mentorship and apprenticeship can help workers develop social relationships and community with peers and supervisors. Additionally, mentors can help workers learn to navigate unspoken rules and norms in the workplace, and assist them with career development within and beyond their current workplace.

RS16. Reduce worker satisfaction

Will the AI system reduce the motivation, engagement, or satisfaction of the workers who use it or are affected by it? While this test directly speaks to meaning, community, and purpose, it is also a proxy for other aspects of worker well-being. Demotivation and disengagement are signs of lowered job satisfaction and serve as indications of other job quality issues.

RS17. Influence employment and pay decisions

Will the AI system make or suggest decisions on recruitment, hiring, promotion, performance evaluation, pay, wage penalties, and bonuses? The decisions outlined in this signal are deeply meaningful to workers, meriting heightened attention from employers. Automation of these decisions should raise concern, as automated systems might lack the complete context necessary for these decisions and risk subjecting workers to “algorithmic cruelty.” They also risk introducing additional discriminatory bases for decisions, beyond those already existent in human decisions. In instances where AI systems are used to suggest (rather than decide) on these questions, careful implementation focused on increasing decision accuracy and transparency can benefit workers. However, human managers using these systems often find it undesirable or difficult to challenge or override recommendations from AI, making the system’s suggestions more binding than they may initially appear and meriting additional caution in these uses.

RS18. Operate in discriminatory ways

Will the AI system operate in ways that are discriminatory? AI systems have been repeatedly shown to reproduce or intensify human discrimination patterns on demographic categories such as gender, race, age, and more. Workplace AI systems should be rigorously tested to ensure that they operate fairly and equitably.
STEP 3
Follow Our Stakeholder-Specific Recommendations

Foster shared prosperity by enacting best practices and suggested uses:

For AI-creating organizations
For AI-using organizations
For policymakers
For labor organizations and workers

Responsible Practices for AI-Creating Organizations (RPC)

Use of workplace AI is still in early stages, and as a result information about what should be considered best practices for fostering shared prosperity is still preliminary. Below is a list for AI-creating organizations of starter sets of practices aligned with increasing the likelihood of benefits to shared prosperity and decreasing the likelihood of harms to it. The list is drawn from early empirical research in the field, historical analogues for transformative workplace technologies, and theoretical frameworks yet to be applied in practice. For ease of use, the lists of Responsible Practices are organized by the earliest AI system lifecycle stage where the practice can be applied.

AT AN ORGANIZATIONAL LEVEL

RPC1. Make a public commitment to identify, disclose, and mitigate the risks of severe labor market impacts presented by AI systems you develop

Multiple AI-creating organizations aspire (according to their mission statements and responsible AI principles) to develop AI that benefits everyone. Very few of them, however, currently publicly acknowledge the scale of labor market disruptions their AI systems might bring about or make efforts to help communities that stand to be affected have a say in the decisions determining the path, depth, and distribution of labor market disruptions. At the same time, AI-creating organizations are often best positioned to anticipate labor market risks well in advance of those becoming apparent to other stakeholders, thus making risk disclosures by AI-creating organizations a valuable asset for governments and societies.
The public commitment to disclose severe risks* should specify the severity threshold considered by the organizations to warrant disclosure, as well as explain how the threshold level of severity was chosen and what external stakeholders were consulted in that decision.

Alternatively, an organization can choose to set a threshold in terms of an AI system’s anticipated capabilities and disclose all risk signals which are present for those systems. For example, if the expected return on investment from the deployment of an AI system is a multiple greater than 10, or more than one million US dollars were spent on training compute and data enrichment, its corresponding risks would be subject to disclosure.*

**DURING THE FULL AI LIFECYCLE**

**RPC2. In collaboration with affected workers, perform Job Impact Assessments early and often throughout the AI system lifecycle**

Run opportunity and risk analyses early and often in the AI research and product development process, using the data available at each stage. Update as more data becomes available (for example, as product-market fit becomes clearer or features are built out enough for broader worker testing and feedback). **Whenever applicable, we suggest using AI system design and deployment choices to maximize the presence of signals of opportunity and minimize the presence of signals of risk.**

Always solicit the input of workers that stand to be affected — both incumbents as well as potential new entrants — and a multi-disciplinary set of third-party experts when assessing the presence of opportunity and risk signals. Make sure to compensate external contributors for their participation in the assessment of the AI system.

Please note that the analysis of opportunity and risk signals suggested here is different from red team analysis suggested in RPC13. The former identifies risks and opportunities created by an AI system working perfectly as intended. The latter identifies possible harms if the AI system in question malfunctions or is misused.

**RPC3. In collaboration with affected workers, develop mitigation strategies for identified risks**

In alignment with UN Guiding Principles for Business and Human Rights, a mitigation strategy should be developed for each risk identified, prioritizing the risks primarily by severity of potential impact and secondarily by its likelihood. Severity and likelihood of potential impact are determined on a case-by-case basis.9

Mitigation strategies can range from eliminating the risk or reducing the severity of potential impact to ensuring access to remedy or compensation for affected groups. If effective mitigation strategies for a given risk are not available, this should be considered a strong argument in favor of meaningful changes in the development plans of an AI system, especially if it is expected to affect vulnerable groups.
Engaging adequately compensated external stakeholders in the development of mitigation strategies is critical to ensure important considerations are not being missed. It is especially critical to engage with representatives of communities that stand to be affected.

**RPC4. Source data enrichment labor responsibly**

Key requirements for the responsible sourcing of data enrichment services (such as, data annotation and real-time human verification of algorithmic predictions) include:

- Always paying data enrichment workers above the local living wage
- Providing clear, tested instructions for data enrichment tasks
- Equipping workers with simple and effective mechanisms for reporting issues, asking questions, and providing feedback on the instructions or task design

In collaboration with our Partners, PAI has developed a [library of practitioner resources](#) for responsible data enrichment sourcing.

**DURING SYSTEM ORIGINATION AND DEVELOPMENT**

**RPC5. Create and use robust and substantive mechanisms for worker participation in AI system origination, design, and development**

Workers who will use or be affected by AI hold unique perspectives on important needs and opportunities in their roles. They also possess particular insight into how AI systems could create harm in their workplaces. To ensure AI systems foster shared prosperity, these workers should be given agency in the AI development process from start to finish.

This work does not stop at giving workers a seat at the table throughout the development process. Workers must be properly equipped with knowledge of product functions, capabilities, and limitations so they can draw meaningful connections to their role-based knowledge. Additionally, care must be taken to create a shared vocabulary on the team, so that technical terms or jargon do not unintentionally obscure or mislead. Workers must also be given genuine decision-making power in the process, allowing them to shape product functions and features, and be taken seriously on the need to end a project if they identify unacceptable harms that cannot be resolved.

**RPC6. Build AI systems that align with worker needs and preferences**

AI systems welcomed by workers largely fall into three overarching categories:

- Systems that directly improve some element of job quality
- Systems that assist workers to achieve higher performance on their core tasks
- Systems that eliminate undesirable non-core tasks (See OS3, RS1, and RS2 for additional detail)

Starting with one of these objectives in mind and creating robust participation mechanisms for workers throughout the design and implementation process is likely to
result in win-win-wins for AI creators, employers who implement AI, and the workers who use or are affected by them.

**RPC7. Build AI systems that complement workers (especially those in lower-wage jobs), not ones that act as their substitutes**

A given AI system complements a certain group of workers if the demand for labor of that group of workers can be reasonably expected to go up when the price of the use of that AI system goes down. A given AI system is a substitute for a certain group of workers if the demand for labor of that group of workers is likely to fall when the price of the use of that AI system goes down.

Note that the terms “labor-augmenting” technology and “labor-complimentary” technology are often erroneously used interchangeably. “Labor-augmenting technology” is increasingly being used as a loose marketing term which frames workplace surveillance technology as worker-assistive.69

Getting direct input from workers is very helpful for differentiating genuinely complementary technology from the substituting kind. Please also see the discussion of the distinction between core and non-core tasks and the acceptable automation thresholds in RS1.

**RPC8. Ensure workplace AI systems are not discriminatory**

In general, AI systems frequently reproduce or deepen discriminatory patterns in society, including ones related to race, class, age, and disability. Specific workplace systems have shown a propensity for the same. Careful work is needed to ensure any AI systems affecting workers or the economy do not create discriminatory results.

**BEFORE SELLING OR DEPLOYING THE SYSTEM**

**RPC9. Provide meaningful, comprehensible explanations of the AI system’s function and operation to workers using or affected by it**

The field of explainable AI has advanced considerably in recent years, but workers remain an underrepresented audience for AI explanations.69 Providing workers explanations of workplace AI systems tailored to the particulars of their roles and job goals enables them to understand the tools’ strengths and weaknesses. When paired with workers’ existing subject matter expertise in their own roles, this knowledge equips workers to most effectively attain the upsides and minimize the downsides of AI systems, meaning AI systems can enhance their overall job quality across the different dimensions of well-being.
RPC10. Ensure transparency about what worker data is collected, how and why it will be used, and enable opt-out functionality

Privacy and ownership over data generated by one’s activities are increasingly rights recognized inside and outside the workplace. Respect for these rights requires fully informing workers about the data collected on them and inferences made, how they are used and why, as well as offering them the ability to opt out of collection and use. Workers should also be given the opportunity to individually or collectively forbid the sales of datasets that include their personal information or personally identifiable information. In particular, system design should follow the data minimization principle: collect only the necessary data, for the necessary purpose, and hold it only for the necessary amount of time. Design should also enable workers to know about, correct, or delete inferences about them. Particular care must be taken in workplaces, as the power imbalance between employer and employee undermines workers’ ability to freely consent to data collection and use compared to other, less coercive contexts.

RPC11. Embed human recourse into decisions or recommendations you offer

AI systems have been built to hire workers, manage them, assess their performance, and promote or fire them. AI is also being used to assist workers with their tasks, coach them, and complete tasks previously assigned to them. In each of these decisions allocated to AI, the technologies have accuracy as well as comprehensiveness issues. AI systems lack the human capacity to bring in additional context relevant to the issue at hand. As a result, humans are needed to validate, refine, or override AI outputs. In the case of task completion, an absence of human involvement can create harms to physical, intellectual, or emotional well-being. In AI’s use in employment decisions, it can result in unjustified hiring or firing decisions. Simply placing a human “in the loop” is insufficient to overcome algorithmic bias: demonstrated patterns of deference to the judgment of algorithmic systems. Care must be taken to appropriately position the strengths and weaknesses of AI systems and empower humans with final decision-making power.

RPC12. Apply additional mitigation strategies to sales and use in environments with low worker protection and decision-making power

AI systems are less likely to cause harm in environments with:

- High levels of legal protection, monitoring, and enforcement for workers’ rights (such as those related to health and safety or freedom to organize)
- High levels of worker voice and negotiating ability (due to strong protections for worker voice or high demand for workers’ comparatively scarce skills), especially those where workers have meaningful input into decisions regarding the introduction of new technologies

These factors encourage worker-centric AI design. Workers in such environments also possess a higher ability to limit harms from AI systems (such as changing elements of an implementation or rejecting the use of the technology as needed), including harms outside
direct legal protections. This should not, however, be treated as a failsafe for harmful technologies, particularly when AI systems can easily be adopted in environments where they were not originally intended. In environments where workers lack legal protection and/or decision-making power, it is especially important to scrutinize uses and potential impacts, building in additional mitigations to compensate for the absence of these worker safeguards. Contractual or licensing provisions regarding terms of use, rigorous customer vetting, and geofencing are some of the many steps AI-creating organizations can take to follow this practice. Care should be taken to adopt fine-grained mitigation strategies where possible such that workers and economies can reap the gains of neutral or beneficial uses.

**RPC13. Red team AI systems for potential misuse or abuse**

The preceding points have focused on AI systems working as designed and intended. Responsible development also requires comprehensive “red teaming” of AI systems to identify vulnerabilities and the potential for misuse or abuse. Adversarial ML is increasingly a part of standard security practice. Additionally, the development team, workers in relevant roles, and external experts should test the system for misuse and abusive implementation.

**RPC14. Ensure AI systems do not preclude the sharing of productivity gains with workers**

The power and responsibility to share productivity gains from AI system implementation lies mostly with AI-using organizations. The role of AI-creating organizations is to make sure the functionality of an AI system does not fundamentally undermine opportunities for workers to share in productivity gains, which would be the case if an AI system de-skills jobs and makes workers more likely to be viewed as fungible or automates a significant share of workers’ core tasks.

**RPC15. Request deployers to commit to following PAI’s Shared Prosperity Guidelines or similar recommendations**

The benefit to workers and society from following these practices can be meaningfully undermined if organizations deploying or using the AI system do not do their part to advance shared prosperity. We encourage developers to make adherence to the Guidelines’ Responsible Practices a contractual obligation during the selling or licensing of the AI system for deployment or use by other organizations.
Responsible Practices for AI-Using Organizations (RPU)

Use of workplace AI is still in early stages, and as a result information about what should be considered best practices for fostering shared prosperity is still preliminary. Below is a list for AI-using organizations of starter sets of practices aligned with increasing the likelihood of benefits to shared prosperity and decreasing the likelihood of harms to it. The list is drawn from early empirical research in the field, historical analogues for transformative workplace technologies, and theoretical frameworks yet to be applied in practice. For ease of use, the lists of Responsible Practices are organized by the earliest AI system lifecycle stage where the practice can be applied.

AT AN ORGANIZATIONAL LEVEL

**RPU1. Make a public commitment to identify, disclose, and mitigate the risks of severe labor market impacts presented by AI systems you use**

Labor practices and impacts are increasingly a part of suggested, proposed, or required non-financial disclosures. These disclosures include practices affecting human rights, management of human capital, and other social and employee issues. Regulatory authorities have suggested, proposed, or required these disclosures as material to investor decision-making, as well as for the benefit of the broader society. We recommend that AI-using organizations identify, disclose, and mitigate the risks of severe labor market impacts for the same rationales, as well as to provide both prospective and existing workers with the information they need to make informed decisions about their own employment.

The public commitment to disclose severe risks should specify the severity threshold considered by the organization to warrant disclosure, as well as explain how the threshold level of severity was chosen and what external stakeholders were consulted in that decision.

Alternatively, an organization can choose to set a threshold in terms of an AI system's marketed capabilities and disclose all risk signals which are present for systems meeting that threshold. For example, if an organization's expected return on investment from the use of an AI system under assessment is a multiple greater than 10, its corresponding risks would be subject to disclosure. In instances where organizational impact is driven by a series of smaller system implementations, the organization could choose to disclose all risk signals present once the cumulative cost decrease or revenue increase exceeds 5%.

---

650
THROUGHOUT THE ENTIRE PROCUREMENT PROCESS, FROM IDENTIFICATION TO USE

**RPU2. Commit to neutrality towards worker organizing and unionization**

As outlined in the signals of risk above, AI systems pose numerous risks to workers’ human rights and well-being. These systems are implemented and used in employment contexts that often have such comprehensive decision-making power over workers that they can be described as “private governments.” As a counterbalance to this power, workers may choose to organize to collectively represent their interests. The degree to which this is protected, and the frequency with which it occurs, differs substantially by location. Voluntarily committing to neutrality towards worker organizing is an important way to ensure workers’ agency is respected and their collective interests have representation throughout the AI use lifecycle if workers so choose (as is repeatedly emphasized as a critical provision in these Guidelines).

**RPU3. In collaboration with affected communities, perform Job Impact Assessments early and often throughout AI system implementation and use**

Run opportunity and risk analyses early and often across AI implementation and use, using the data available at each stage. Update as more data becomes available (for example, as objectives are identified, systems are procured, implementation is completed, and new applications arise). Whenever applicable, we suggest using AI system implementation and use choices to maximize the presence of signals of opportunity and minimize the presence of signals of risk.

Solicit the input of workers that stand to be affected and a multi-disciplinary set of independent experts when assessing the presence of opportunity and risk signals. Make sure to compensate external contributors for their participation in the assessment of the AI system.

Please note that the analysis of opportunity and risk signals suggested here is different from red team analysis suggested in RPU15. The former identifies risks and opportunities created by an AI system working perfectly as intended. The latter identifies possible harms if the AI system in question malfunctions or is misused.

**RPU4. In collaboration with affected communities, develop mitigation strategies for identified risks**

In alignment with UN Guiding Principles for Business and Human Rights, a mitigation strategy should be developed for each risk identified, prioritizing the risks primarily by severity of potential impact and secondarily by its likelihood. Severity and likelihood of potential impact are determined on a case-by-case basis.

Mitigation strategies can range from eliminating the risk or reducing the severity of potential impact to ensuring access to remedy or compensation for affected groups.

---

U It is frequently the case that workers who stand to be affected by the introduction of an AI system include not only workers directly employed by the organization introducing AI in its own operations, but a wider set of current or potential labor market participants. Therefore it is important that not only incumbent workers are given the agency to participate in job impact assessment and risk mitigation strategy development.

V An algorithm described here is very useful for determining the severity of potential quantitative impacts (such as impacts on wages and employment), especially in cases with limited uncertainty around the future uses of the AI system being assessed.
If effective mitigation strategies for a given risk are not available, this should be considered a strong argument in favor of meaningful changes in the development plans of an AI system, especially if it is expected to affect vulnerable groups.

Engaging workers and external experts as needed in the creation of mitigation strategies is critical to ensure important considerations are not being missed. It is especially critical to engage with representatives of communities that stand to be affected. Please ensure that everyone engaged in consultations around assessing risks and developing mitigation strategies is adequately compensated.

**RPU5. Create and use robust and substantive mechanisms for worker agency in identifying needs, selecting AI vendors and systems, and implementing them in the workplace**

Workers who will use or be affected by AI hold unique perspectives on important needs and opportunities in their roles. They also possess particular insight into how AI systems could create harm in their workplaces. To ensure AI systems foster shared prosperity, these workers should be included and afforded agency in the AI procurement, implementation, and use process from start to finish.

Workers must be properly equipped with knowledge of potential product functions, capabilities, and limitations, so that they can draw meaningful connections to their role-based knowledge (see RPU13 for more information). Additionally, care must be taken to create a shared vocabulary on the team, so that technical terms or jargon do not unintentionally obscure or mislead. Workers must also be given genuine decision-making power in the process, allowing them to shape use (such as new workflows or job design) and be taken seriously on the need to end a project if they identify unacceptable harms that cannot be resolved.

**RPU6. Ensure AI systems are used in environments with high levels of worker protections and decision-making power**

AI systems are less likely to cause harm in environments with:

- High levels of legal protection, monitoring, and enforcement for workers’ rights (such as those related to health and safety or freedom to organize)
- High levels of worker voice and negotiating ability (due to strong protections for worker voice or high demand for workers’ comparatively scarce skills), especially those where workers have meaningful input into decisions regarding the introduction of new technologies

These factors encourage worker-centric AI design. Workers in such environments also possess a higher ability to limit harms from AI systems (such as changing elements of an implementation or rejecting the use of the technology as needed), including harms outside direct legal protections. This should not, however, be treated as a failsafe for harmful technologies: other practices in this list should also be followed to reduce risk to workers.
**RPU7. Source data enrichment labor responsibly**

Key requirements for the responsible sourcing of data enrichment services (such as, data annotation and real-time human verification of algorithmic predictions) include:

- Always paying data enrichment workers above the local living wage
- Providing clear, tested instructions for data enrichment tasks
- Equipping workers with simple and effective mechanisms for reporting issues, asking questions, and providing feedback on the instructions or task design

In collaboration with our Partners, PAI has developed a library of practitioner resources for responsible data enrichment sourcing.

**RPU8. Ensure workplace AI systems are not discriminatory**

In general, AI systems frequently reproduce or deepen discriminatory patterns in society, including ones related to race, class, age, and disability. Specific workplace systems have shown a propensity for the same. Careful vetting and use is needed to ensure any AI systems affecting workers or the economy do not create discriminatory results.

**WHEN IDENTIFYING NEEDS, PROCURING, AND IMPLEMENTING AI SYSTEMS**

**RPU9. Procure AI systems that align with worker needs and preferences**

AI systems welcomed by workers largely fall into three overarching categories:

- Systems that directly improve some element of job quality
- Systems that assist workers to achieve higher performance on their core tasks
- Systems that eliminate undesirable non-core tasks (See OS2, OS9, RS1, and RS2 for additional detail)

Starting with one of these objectives in mind and creating robust participation mechanisms for workers throughout the design and implementation process is likely to result in win-win-wins for AI creators, employers who implement AI, and the workers who use or are affected by them.

**RPU10. Staff and train sufficient internal or contracted expertise to properly vet AI systems and ensure responsible implementation**

As discussed throughout, AI systems raise substantial concerns about the risks of their adoption in workplace settings. To understand and address these risks, experts are needed to vet and implement AI systems. In addition to technical experts, this includes sociotechnical experts capable of performing the Job Impact Assessment described above to the level of granularity necessary to fully identify and mitigate risks of a specific system in a given workplace.

The importance of this practice increases with AI system customization or integration. In situations where systems are developed by organizations who follow the Shared Prosperity
Guidelines or similar recommendations, disclose potential labor impacts, and design these systems to be used off-the-shelf, less internal expertise may be required from users. However, when systems are more customized or integrated into workplaces, specifics related to the organization and worksite more heavily influence labor impacts arising from the particulars of system use, requiring additional expertise.

**RPU11. Prefer vendors who commit to following PAI’s Shared Prosperity Guidelines or similar recommendations**

The benefit to workers and society from following these practices can be meaningfully undermined if organizations designing and selling the AI system do not do their part to advance shared prosperity. We encourage users to make developer adherence to PAI’s Guidelines or similar recommendations a priority when selecting vendors and systems for use.

**RPU12. Ensure transparency about what worker data is collected, how it will be used, and why, and enable workers to opt out**

Privacy and ownership over data generated by one’s activities are increasingly rights recognized inside and outside the workplace. Respect for these rights requires fully informing workers about the data collected on them and inferences made, how they are used and why, as well as offering them the ability to opt out of collection and use. Workers should also be given the opportunity to individually or collectively forbid the sales of datasets that include their personal information or personally identifiable information. Depending on use, generative AI may present novel privacy risks, through extracting information about worker practices and sharing with managers and colleagues. System design and use should follow the data minimization principle: collect only the necessary data, for the necessary purpose, and hold it only for the necessary amount of time. Design should also enable workers to know about, correct, or delete inferences about them.

Particular care must be taken in workplaces, as the power imbalance between employer and employee undermines workers’ ability to freely consent to data collection and use compared to other, less coercive contexts. In practice, data use decisions by employers often shift over time, making it especially important for AI-using organizations to explicitly and transparently inform workers regarding each new use of their data and its implications, and request consent for each new use or repurposing.

**RPU13. Provide meaningful, comprehensible explanations of the AI system’s function and operation to workers overseeing it, using it, or affected by it**

The field of explainable AI has advanced considerably in recent years, but workers remain an underrepresented audience for AI model explainability efforts. Providing managers and workers explanations of workplace AI systems tailored to the particulars of their roles and job goals enables them to understand the tools’ strengths and weaknesses. When paired
with workers’ existing subject matter expertise in their own roles, this knowledge equips managers and workers to most effectively attain the upsides and minimize the downsides of AI systems, meaning AI systems can enhance overall job quality across the different dimensions of well-being.

**RPU14. Establish human recourse into decisions or recommendations offered, including the creation of transparent, human-decided grievance redress mechanisms**

AI systems have been built to hire workers, manage them, assess their performance, and promote or fire them. AI is also being used to assist workers with their tasks, coach them, and complete tasks previously assigned to them. In each of these decisions allocated to AI, the technologies have accuracy as well as comprehensiveness issues. AI systems lack the human capacity to bring in additional context relevant to the issue at hand. As a result, humans are needed to validate, refine, or override AI outputs. In the case of task completion, an absence of human involvement can create harms to physical, intellectual, or emotional well-being. In AI’s use in employment decisions, it can result in unjustified hiring or firing decisions. Simply placing a human “in the loop” is insufficient to overcome algorithmic bias: demonstrated patterns of deference to the judgment of algorithmic systems. Care must be taken to appropriately position the strengths and weaknesses of AI systems and empower humans with final decision-making power.

**RPU15. Red team AI systems for potential misuse or abuse**

The preceding points have focused on AI systems working as designed and intended. Responsible development also requires comprehensive “red teaming” of AI systems to identify vulnerabilities and the potential for misuse or abuse. Managers, workers in relevant roles, and external experts should test the system for misuse and abusive implementation.

**RPU16. Recognize extra work created by AI system use and ensure work is acknowledged and compensated**

The above practice of red-teaming addresses intentional misuse or abuse. More routinely, AI systems fail to work as marketed or intended in ways big and small, creating additional tasks for workers to absorb. New tasks generated by the gap between AI system expectations and realities often go unrecognized, leaving workers to shoulder extra responsibilities or work without providing them additional time to complete these tasks or compensation for doing so. Address this issue by holding routine reviews with the workers who use or oversee systems to identify areas of new work and adjust accordingly.
**RPU17. Ensure mechanisms are in place to share productivity gains with workers**

The power and responsibility to share productivity gains from AI system implementation lies largely with AI-using organizations. AI-using organizations hold final decisions about wages, benefits, working hours, job design, worker retraining and reskilling, and more. To the extent that AI systems deliver cost savings and/or higher revenues via increased worker productivity, AI-using organizations hold authority over how to allocate increased margins. As highlighted in OS7, AI systems present a major opportunity to improve workers’ well-being, financial and otherwise, through maintaining or increasing their share of revenue without decreasing absolute returns to owners or shareholders.
Suggested Uses for Policymakers

We currently anticipate two primary ways in which the Guidelines can be used by policymakers, described below. If you have feedback, suggestions, or would like to explore using the Guidelines in your work, please get in touch.

1. Policymakers can integrate the Job Impact Assessment steps suggested by the Guidelines into existing or emerging standards, risk management frameworks, and conformity assessments to encourage AI-creating and AI-using organizations to assess and disclose their anticipated impacts on shared prosperity and abide by Responsible Practices suggested by the Guidelines. This can be done either as a part of “horizontal” or sectoral AI regulation or by making existing worker protection laws better fit the age of rapid adoption of AI throughout the economy.

2. Policymakers can perform the Job Impact Assessment Tool’s risk and opportunities analysis themselves to better identify the possible impacts of AI uses of interest on shared prosperity. Such analysis can be relevant in multiple contexts, including:
   - Considering the need for new regulation or modification of existing regulation in light of emergence of new uses of AI
   - Informing good jobs creation strategy at the local, regional, or state level
   - Making decisions about whether to provide tax breaks or other incentives to attract specific industries into the region with the goal of strengthening the local labor market
   - Ensuring sustainability of social protection mechanisms in the context of changing technological landscape, anticipating the pace and timing of increases in unemployment benefits claims, and declines in labor income tax revenue.
**Suggested Uses for Labor Organizations and Workers**

We currently anticipate four ways in which the Guidelines can be used by unions, worker organizations, worker representatives, and workers, described below. If you have feedback, suggestions, or would like to explore using the Guidelines in your work, please get in touch.

1. The Job Impact Assessment Tool and Responsible Practices can be used to audit or assess existing or prospective AI systems and offer a foundation for dialogue or negotiation over system need identification, purchases, implementation, and use. Such dialogues or negotiations could consider existing or potential impacts on workers, as well as transparency and consent in workplace data collection and use. Where opportunities exist for workers and their representatives to have agency in AI system design, the tools provided in the Guidelines can be used to identify areas for further analysis and improvement.

2. The Guidelines offer ideas for potential provisions to be included in collective bargaining agreements or other mechanisms for advancing employer workplace policies. Some jurisdictions explicitly delineate technology as an area for collective worker input and decision-making, while in others it is voluntary. Not all signals or responsible practices will be applicable to all AI systems or workplaces, but they can serve as an inventory for negotiators to include or draw inspiration from as they consider risks in their own workplaces.

3. The Guidelines outline issues that unions and worker organizations may wish to cover in trainings or educational sessions with members. The Job Impact Assessment Tool offers guidance on potential harms to watch out for, as well as possible benefits that workers can advocate for. Additionally, familiarizing workers with the Responsible Practices for AI-using organizations can equip them for advocacy for better workplace AI use within their teams, worksites, or organizations.

4. The Guidelines can be used to inform positions in policy discussions. As unions and worker organizations consider their policy objectives and goals, this tool can support informed engagement to shape the future of work.
Acknowledgements

The content of the Guidelines was iteratively developed by PAI’s Labor and Economy team (Katya Klinova, Stephanie Bell, and Sonam Jindal) under comprehensive guidance of the AI and Shared Prosperity Initiative’s Steering Committee. We thank the Steering Committee members for their steadfast commitment to the work of the Initiative and their generosity in investing their time, expertise, and effort to advance this effort.

We thank the frontline workers in the US, India, and Sub-Saharan Africa whose participation centrally informed the content of the Guidelines. We are grateful to Andre Barbe and Albert Tanjaya for excellent research support, and to Hudson Hongo and Neil Uhl for their thought partnership, crucial editorial support, and user experience design. We thank all past and present PAI colleagues and Partners who enabled and supported the work of the Initiative from its inception. We thank Ed Bayes, Elaine Chang, and Christina Colclough, for reviewing early drafts of the Guidelines and providing valuable feedback.

We are grateful to the Ford Foundation’s Future of Work(ers) Program for financial support of the AI and Shared Prosperity Initiative, and personally to Ritse Erumi for valuable support and guidance.

The Guidelines build on the work of many exceptional scholars and advocates cited throughout this document. We are deeply grateful for their leadership.
AI and Shared Prosperity Initiative’s Steering Committee

Abbie Langston, Director, Equitable Economy at PolicyLink

Aiha Nguyen, Program Director, Labor Futures Initiative at Data & Society Research Institute

Andrea Dehlendorf, Senior Advisor and Co-Founder at United for Respect

Andrew Kortina, Co-founder of Venmo and Fin.com

Anton Korinek, Professor of Economics at University of Virginia and David M. Rubenstein Fellow at the Brookings Institution

Arturo Franco, Senior Vice President, Center for Inclusive Growth at Mastercard

Damon Silvers, Senior Advisor at AFL-CIO

Daron Acemoglu, Institute Professor of Economics at MIT

Dean Carignan, Senior Director of Product Management, Office of the Chief Scientist at Microsoft

Deborah Greenfield, Former Deputy Director-General for Policy at the International Labour Organization

Dunstan Allison-Hope, Vice President at Business for Social Responsibility

Grace Mutung’u, Research Fellow, Centre for Intellectual Property & Information Technology at Strathmore University

Jessica Fulton, Vice President at the Joint Center for Political & Economic Studies

Jody Medich, CEO, Founder at Superhuman-X

Jordan Usdan, Senior Director, Strategy & Innovation, Office of the CTO at Microsoft

Juana Catalina Becerra Sandoval, Visiting Scholar, Responsible & Inclusive Tech at IBM

Lama Nachman, Intel Fellow & Director, Anticipatory Computing Lab at Intel

Pamela Mishkin, Policy Staff Member at OpenAI

Rahul Panicker, Head of Product, Robotics Applications at Intrinsic

Reema Nanavaty, Executive Director at Self Employed Women’s Association

Ryan Gerety, Acting Director at Athena Coalition

Sarah Treuhaft, Senior Director of Policy and Partnerships at the Institute on Race, Power, and Political Economy

Shakir Mohamed, Senior Staff Scientist at DeepMind
“Without an explicit intention to develop and use artificial intelligence toward enhancing the livelihoods of all of us, it will accelerate and reinforce the most unequal power dynamics in our society. These Guidelines reflect the field’s current best thinking on evaluating whether a particular use enhances shared prosperity or fuels wealth concentration off the backs of working people. We hope to use these Guidelines together with workers to evaluate corporate employer practices and fight for better working conditions.”

United for Respect

“AI has enormous potential to change how we work and—like any powerful technology—must be deployed responsibly and incorporate feedback from a wide variety of stakeholders. We welcome the Guidelines as an important step in ensuring AI benefits all of humanity, and we are pleased to work with PAI to help refine and operationalize these guidelines to help ensure that everyone can share in the economic prosperity unleashed by new AI technologies.”

Pamela Mishkin
Policy Staff Member, OpenAI

“I highly recommend the Guidelines for AI and Shared Prosperity for AI developers and deployers. It’s our responsibility to assess the economic and job quality impacts of our innovations. With these tools, we can make well-informed choices and avoid causing more harm than good.”

Anton Korinek
Professor of Economics, University of Virginia

“Developing AI that genuinely complements workers and improves business processes is a difficult challenge we’ve been working hard on at Intel. The Guidelines for AI and Shared Prosperity are a helpful resource on that journey. I’m glad to have guided their development and look forward to helping test the Guidelines—I encourage leaders and researchers at other AI companies to join this effort.”

Lama Nachman
Intel Fellow & Director, Anticipatory Computing Lab, Intel

“Our decisions about how to develop, use, and govern AI will reshape our society and determine who benefits and who is left behind. PAI’s strong research, stakeholder engagement, and practical guidelines are all essential tools for policymakers, developers, and companies adopting these technologies, to ensure that they truly complement human effort. We can build a world that balances productivity with opportunity.”

Arturo Franco
Senior Vice President, Mastercard Center for Inclusive Growth
“A just society would not allow AI systems to degrade job quality and wages for the most marginalized workers in the name of greater efficiency and growth that benefits the already-prosperous. I applaud PAI’s Guidelines for AI and Shared Prosperity for prioritizing the needs of workers with the least power to protect themselves from AI harms. The Guidelines are a crucial resource for policymakers, civil society, labor organizers, and anyone else interested in ensuring AI creates equitable outcomes for all workers.”

Sarah Treuhaft
Senior Director of Policy and Partnerships, Institute on Race, Power, and Political Economy

“I’m delighted that the Shared Prosperity Guidelines include recommendations for “AI using organizations” in addition to “AI creating organizations”. Companies deploying AI systems make essential choices that determine the impact of AI on jobs and workers, and these Guidelines provide a new and much-needed resource for responsible AI governance and decision making.”

Dunstan Allison-Hope
Vice President, Business for Social Responsibility

“A future of work that embraces technology as a tool for equitable, inclusive and sustainable growth depends upon efforts like PAI’s Guidelines for AI and Shared Prosperity. The initiative’s worker-centered foundation provides a powerful tool for trade unions and other advocates to understand the promises and risks of AI, engage in meaningful dialogue with those who develop and disseminate it, and harness its power on behalf of labor.”

Deborah Greenfield
Former Deputy Director-General for Policy, International Labour Organization

“Without swift and careful action, artificial intelligence may cause substantial harms to workers around the globe. I welcome the release of PAI’s Guidelines for AI & Shared Prosperity, and appreciate their focus on ensuring AI will have positive impacts for all workers, including workers in low- and middle-income countries. The Guidelines are an essential tool for any AI-developing or AI-using company, and offer helpful guidance for policymakers, workers, unions, and civil society around the world.”

Grace Mutung’u
Centre for Intellectual Property & Information Technology at Strathmore University

“If corporations productively deploy AI, they’ll see a boost in the efficiency of information work processes. Given corporate incentive structures and (lack of) retraining agility, the easiest way to realize benefits of improved efficiency will be through a reduction in workforce size. I hope some policy makers are anticipating this possibility and evaluating ways to redistribute corporate profits to workers who will consequently need to search for new jobs or new industries.”

Andrew Kortina
Co-founder, Venmo & fin.com
“Today, over 60% of the workforce globally and over 90% of the workforce in the Global South countries is in the informal economy. These workers generally form the bottom and the lower-middle sector of the global value chains where the risks are concentrated. Emerging technologies like AI are going to have maximum effect on the jobs of these workers—displacing them, pushing them out of the workforce, making their existing skills redundant. These Guidelines will serve as an important tool for these poor informal sector workers and their organizations to prepare them for the upcoming impacts of AI and help build their resilience against the changing world of work.”

Reema Nanavaty
Director, Self Employed Women’s Association (SEWA)

“New technological and AI tools in the workplace are having an undeniable impact on workers and industries, from low-wage gig work to creative industries like film and journalism. However, the public discourse has been dominated by stories of the inevitability of technology and not enough attention has been placed on the decisions that went into getting us to this point, namely who gets to reap the benefits and who assumes the risks? The Guidelines for AI and Shared Prosperity offer an opportunity for all stakeholders to make transparent how those risks and benefits are allocated, and reflect or even change on those decisions, because this is how we have a real dialogue about the benefits of AI.”

Aiha Nguyen
Program Director, Labor Futures Initiative Data & Society Research Institute

“The Partnership on AI has done an outstanding job developing these important recommendations for how we as a society should deploy AI so that it can benefit all. These practical and commonsense guidelines for developers of AI, impacted companies and workers, and policy makers, are an important step towards ensuring true shared prosperity.”

Rahul Panicker
Head of Product, Robotics Applications, Intrinsic
Sources


37 Pritchett, L. (2020). The future of jobs is facing one, maybe two, of the biggest price distortions ever. Middle East Development Journal, 12(1), 131-156.


54 (Center for Democracy & Technology et al. 2022)


## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>The need for workers' perspectives on workplace AI</td>
<td>6</td>
</tr>
<tr>
<td>The contributions of this report</td>
<td>8</td>
</tr>
<tr>
<td>Our approach</td>
<td>9</td>
</tr>
<tr>
<td>Key research questions</td>
<td>9</td>
</tr>
<tr>
<td>Research methods</td>
<td>9</td>
</tr>
<tr>
<td>Site selection</td>
<td>9</td>
</tr>
<tr>
<td>Who we learned from</td>
<td>11</td>
</tr>
<tr>
<td>Participant recruitment</td>
<td>12</td>
</tr>
<tr>
<td><strong>Major Themes and Findings</strong></td>
<td>13</td>
</tr>
<tr>
<td>Theme 1: Executive and managerial decisions shape AI's impacts on workers, for better and worse</td>
<td>13</td>
</tr>
<tr>
<td>Theme 2: Workers appreciate how some uses of AI have positively changed their jobs</td>
<td>16</td>
</tr>
<tr>
<td>Theme 3: Workplace AI harms repeat, continue, or intensify known possible harms from earlier technologies</td>
<td>18</td>
</tr>
<tr>
<td>Theme 4: Current implementations of AI in work are reducing workers' opportunities for autonomy, judgment, empathy, and creativity</td>
<td>20</td>
</tr>
<tr>
<td>Theme 5: Empowering workers early in AI development and implementation increases opportunities to implement AI that benefits workers as well as their employers</td>
<td>22</td>
</tr>
<tr>
<td><strong>Opportunities for Impact</strong></td>
<td>24</td>
</tr>
<tr>
<td>Stakeholder 1: AI-implementing companies</td>
<td>25</td>
</tr>
<tr>
<td>Stakeholder 2: AI-creating companies</td>
<td>26</td>
</tr>
<tr>
<td>Stakeholder 3: Workers, unions, and worker organizers</td>
<td>28</td>
</tr>
<tr>
<td>Stakeholder 4: Policymakers</td>
<td>29</td>
</tr>
<tr>
<td>Stakeholder 5: Investors</td>
<td>31</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>32</td>
</tr>
<tr>
<td><strong>Acknowledgments</strong></td>
<td>33</td>
</tr>
<tr>
<td><strong>The AI and Shared Prosperity Initiative Steering Committee</strong></td>
<td>34</td>
</tr>
<tr>
<td><strong>Appendices</strong></td>
<td>35</td>
</tr>
<tr>
<td>Appendix 1: Detailed site and technology descriptions</td>
<td>36</td>
</tr>
<tr>
<td>Appendix 2: Research methodology</td>
<td>40</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>44</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1  Research & insight creation approach  
Figure 2  Stages of employee lifecycle/worker journey where AI tools may be implemented  
Figure 3  Participant demographics & characteristics: Overall  
Figure 4  AI technology types included in study by worker journey stage and site  
Figure 5  Participant demographics & characteristics: India  
Figure 6  Participant demographics & characteristics: Sub-Saharan Africa  
Figure 7  Participant demographics & characteristics: United States
Executive Summary

Across industries and around the world, AI is changing work. In the coming years, this rapidly advancing technology has the potential to fundamentally reshape humanity’s relationship with labor. As highlighted by previous Partnership on AI (PAI) research, however, the development and deployment of workplace AI often lacks input from an essential group of experts: the people who directly interact with these systems in their jobs.

Bringing the perspectives of workers into this conversation is both a moral and pragmatic imperative. Despite the direct impact of workplace AI on them, workers rarely have direct influence in AI's creation or decisions about its implementation. This neglect raises clear concerns about unforeseen or overlooked negative impacts on workers. It also undermines the optimal use of AI from a corporate perspective.

This PAI report, based on an international study of on-the-job experiences with AI, seeks to address this gap. Through journals and interviews, workers in India, sub-Saharan Africa, and the United States shared their stories about workplace AI. From their reflections, PAI identified five common themes:

1. Executive and managerial decisions shape AI’s impacts on workers, for better and worse. This starts with decisions about business models and operating models, continues through technology acquisitions and implementations, and finally manifests in direct impacts to workers.

2. Workers have a genuine appreciation for some aspects of AI in their work and how it helps them in their jobs. Their spotlights here point the way to more mutually beneficial approaches to workplace AI.

3. Workplace AI’s harms are not new or novel — they are repetitions or extensions of harms from earlier technologies and, as such, should be possible to anticipate, mitigate, and eliminate.

4. Current implementations of AI often serve to reduce workers’ ability to exercise their human skills and talents. Skills like judgment, empathy, and creativity are heavily constrained in these implementations. To the extent that the future of AI is intended to increase humans’ ability to use these talents, the present of AI is sending many workers in the opposite direction.

5. Empowering workers early in AI development and implementation increases the opportunities to attain the aforementioned benefits and avoid the harms. Workers’ deep experience in their own roles means they should be treated as subject-matter experts throughout the design and implementation process.
In addition, PAI drew from these themes to offer opportunities for impact for the major stakeholders in this space:

1. AI-implementing companies, who can commit to AI deployments that do not decrease employee job quality.
2. AI-creating companies, who can center worker well-being and participation in their values, practices, and product designs.
3. Workers, unions, and worker organizers, who can work to influence and participate in decisions about technology purchases and implementations.
4. Policymakers, who can shape the environments in which AI products are developed, sold, and implemented.
5. Investors, who can account for the downside risks posed by practices harmful to workers and the potential value created by worker-friendly technologies.

The actions of each of these groups have the potential to both increase the prosperity enabled by AI technologies and share it more broadly. Together, we can steer AI in a direction that ensures it will benefit workers and society as a whole.
Introduction

The need for workers’ perspectives on workplace AI

In the past decade, global investment in artificial intelligence development has soared. Private investment in AI went from under $5 billion globally in 2013 to over $90 billion in 2021, more than doubling between 2020 and 2021 alone. The implementation of AI products has similarly grown: In 2021, 56% of respondents to a McKinsey survey said their organizations used AI in at least one business function compared to 20% of respondents in 2017 who reported using AI at scale or in a core part of their business. The positive and negative effects of this are already being felt by both formal workers (millions of whom are interacting with AI products or will soon see them incorporated into their jobs) and informal workers (who are encountering transformed market conditions due to the use of AI by businesses). For both groups of workers, the positive and negative impacts of these technologies are unevenly distributed, often following other existing axes of inequality, such as geography, race, and gender. Yet workers’ needs, well-being, and expertise are under-considered in AI research, development, and implementation.

In an earlier publication, “Redesigning AI for Shared for Prosperity: An Agenda,” PAI highlighted the need to better understand AI’s impacts on job quality, including by engaging the workers who experience these impacts firsthand. Workers who directly interact with AI understand these systems’ benefits and harms in depth. In the best of circumstances, they experience the ways these technologies can make their work more efficient, error-free, and pleasurable or less grueling, tiring, or dangerous. Too frequently, workers also experience the downsides. These systems can restrict workers’ autonomy, invade their privacy, undercut their judgment and empathy, and push them to the point of exhaustion or injury. Companies that allocate managerial tasks to AI systems can subject workers to binding decisions that are capricious or cruel.

At a societal level, the increasing adoption of AI systems is poised to accelerate existing problems arising from economic inequality. AI research and product development is taking place in a highly concentrated group of countries and companies. Private AI investment in the United States in 2021 totaled $52.9 billion, over three times the investment by the next highest country, China at $17.2 billion — which in turn exceeded investment by the next nine countries combined. The impacts of workplace AI use, however, will be felt around the world. As some companies attempt to automate work they had previously outsourced, others will adopt AI systems created in and for entirely different geographies. Both between and within countries, AI’s current trajectory threatens to widen the gaps between the haves and have-nots.
Moreover, workers are uniquely positioned to understand how to avoid these harms and contribute ideas to improve their employers’ bottom lines. Using AI to increase job quality (or at least not decrease it) would enable employers to reap the benefits of a more engaged and satisfied workforce. Higher job quality and employee satisfaction increases productivity of existing workers, reduces turnover (retaining experience and expertise), and fosters the ability to recruit higher-caliber talent in competitive labor markets. Decades of research on innovation in domains as diverse as manufacturing, hospitality, and government service provision has underscored the unique insights and innovative potential of frontline workers and other individual contributors. Workers are afforded intimate knowledge of crucial aspects of their work that managers and leaders only see from a distance. They are experts in things like the nuances of how to create the conditions for customer satisfaction or the levels of care that need to be taken in moving objects of different fragility through a warehouse. This deep knowledge of the ins and outs of completing core tasks makes workers an underutilized source of expertise on issues and problems where AI could be a powerful tool or assistant.

Finally, pursuing collaborative workplace AI that draws on the unique strengths of humans and technology enables businesses to expand the production frontier. Many current integrations of AI into human workflows are designed around the limited capabilities of the AI systems. This, in turn, circumscribes the range of talents and skills of the people who work with them. Starting from the opposite premise — that AI should be integrated into workplaces in a way that enables human skills and talents to flourish — is undeniably harder. The reward for the achievement, however, is far greater for both workers and their employers.

**WHY WON’T THE MARKET ADDRESS HARMs BY INCREASING WAGES?**

Strict rationalist economic theory would predict that workers will receive sufficient wages to compensate for technologically driven harms. However, employers and workers alike lack the perfect information required for this effect. Additionally, this theory presumes robust competition for labor, and workers who possess a genuine ability to choose between different employment options. In many labor markets, employment options are relatively concentrated, enabling companies to treat workers worse than they would in more competitive environments. Steps to increase information and awareness can reduce the likelihood that workers unwittingly accept poor working conditions without a sufficient compensating wage. Regulation and increased unionization can reduce the negative effects of concentrated labor markets. However, the insufficiency (as well as improbability) of these solutions point to a need for direct attention to AI’s effects on job quality.
The contributions of this report

Past research and discussions on AI's impacts on workers have frequently taken one of three forms, with the first two especially common in popular and business discussions:

1. Predictions about AI's impacts on job availability (i.e., how many jobs AI will eliminate and which ones).
2. Aspirational discussions of how AI will improve work for humans by automating “dull, dirty, and dangerous” work.
3. Targeted research by academics and civil society groups on the negative impacts of AI focused on specific technologies or groups of workers.

In this last category, groundbreaking research has illuminated the harms of specific AI technologies and use cases, including monitoring and surveillance, algorithmic decision-making, shift-scheduling, and platform work software and applications. Researchers have also explored particular types of impacts on workers, including worker health and safety, data collection and privacy, and reproductions of carceral power.

Previously, PAI itself conducted a landscape review of AI’s demonstrated and potential impacts on worker well-being.

This report builds on this foundational work by bringing in the perspectives and experiences of frontline workers at the frontier of workplace AI implementation around the world. It shares their stories of how their jobs have been transformed by AI (for better and for worse) and highlights their oft-neglected expertise on challenges and opportunities in their work where they welcome AI assistance. It also synthesizes this primary research with the existing literature to offer implications and opportunities for key stakeholders on how they can take action to ensure the category of technological products commonly referred to as AI improves — not worsens — the experience of workers. Finally, it offers areas in need of further exploration in future research or implementation case studies.

Through their comments and stories, workers surfaced five key themes about their experiences of AI in the workplace. These five themes point the way toward a better future for workplace AI, one that maintains or increases companies’ profitability and revenue while also maintaining or increasing job quality. Getting there will require many decision-makers and stakeholders to do things differently than they have in the past. In some instances, the needed changes are substantial and complex. At the end of this report, we offer initial recommendations for all of the major stakeholders in this space: AI-using companies, AI-creating companies, workers and the organizations such as unions that represent them, policymakers, and investors.
Our approach

Key research questions

We set out to understand workers’ experience of AI in their jobs and possible opportunities to foster worker participation and voice in the processes of AI creation and deployment. Our key research questions were:

- How and why are AI and automation technologies changing workers’ tasks, coaching, and evaluation? What are workers’ reflections on the positives and negatives of those changes?
- How is workplace AI affecting different aspects of worker well-being (including purpose, meaning, and physical, emotional, and intellectual well-being) as articulated and valued by workers themselves?
- In what ways are workers currently participating in the creation and implementation of AI used in their workplaces? How much direct influence or decision-making power do they see themselves as having in these processes? Would they be interested in more ways to participate? Why or why not?

Research methods*

The findings of this report are grounded in a review of the existing research and two types of primary qualitative research we conducted with workers: diary studies and interviews. All primary research was conducted virtually due to the pandemic.

Figure 1: Research & insight creation approach

1. Literature review
   - Review existing academic and civil society research, identify impact areas with low coverage & opportunities to add actionable detail

2. Diary studies
   - Asynchronously solicit near-real-time, less-mediated storytelling from participants on how AI has transformed their jobs

3. Interviews
   - Conduct semi-structured interviews to expand upon and test emerging themes, explore outlier responses and views

4. Analysis
   - Deductive technology use clustering, inductive job quality theme analysis

Site selection*

AI’s transformation of work is global in scope. Its impacts within and across countries often follow deeply grooved paths of inequality created by past economic and political systems. We conducted the primary research with three groups of workers, focusing on people holding individual contributor (rather than managerial) roles:

- Customer service agents in India
- Data annotators in sub-Saharan Africa
- Warehouse workers (e.g., pickers, packers, loaders) in the United States
We sought a range of geographies, industries, occupations, and skills. This multisite approach allowed us to explore diverse experiences on issues including:

- Whether there is something inherent to artificial intelligence as a technology (irrespective of geography, industry, and worker skills) in how it transforms work
- The economic opportunities and vulnerabilities associated with varying wage and income levels (between different occupations and geographies)
- Worker attitudes toward jobs and labor
- Labor market structures and near-term susceptibility to technological disruption by AI
- Managerial decision-making cultures
- Government interest in fostering local AI ecosystems
- Government interest and capacity to regulate AI’s impacts on workers  

While workers may be affected by AI technologies across the “employee lifecycle,” this research focuses on use cases where workers could directly observe AI in their workplace and thus share their experiences of it. In line with this approach, this report also discusses different technologies as experienced by the participating workers, in what might be thought of as the “worker’s journey” in a given job. As an illustration, a technology used by an employer to provide guidance to workers on their tasks is discussed as a worker’s coaching tool, not as a manager’s automation or decision-support tool.

Workers largely encountered the AI technologies described in this study in three stages of their jobs: in their fulfillment of their roles, to coach them on their work, or to evaluate their performance.
Who we learned from

The occupations and locations selected feature workers representing a diversity of profiles. In India, offshore call center work is a stable, middle-class job often performed by college-educated workers fluent in a second language (in this case, English). Shifts are scheduled according to the needs of the outsourcing country, so workers often find themselves working night shifts, very early, or very late to match standard working hours in high-income English-speaking countries around the world. These hours are hard to navigate alongside family life; it is estimated that over 90% of people in these roles are under the age of 35.47

The data annotation workers in the sub-Saharan country where this research was conducted are similarly youthful. This work is often positioned as an entry-level job for those interested in the continent’s growing information technology industry. As educational requirements are less strict than those for offshore customer service workers in India, educational backgrounds are more varied. Most workers have at least a secondary school degree and many have gone on to take classes in or complete post-secondary or bachelor’s degrees.

Unlike in the other two sites, the demographic profile of warehouse workers in the United States is highly heterogeneous. The purpose of the work means worksites are distributed throughout the country rather than concentrated in a handful of cities or a region. Substantial skill or education requirements are uncommon for entry-level jobs in the industry. Given the US’s history of education inequality and the lack of access to quality education for many people of color, people of color are overrepresented in warehouse work in the US, making up nearly 60% of the industry workforce.48
**Participant recruitment**

Participants for this research were recruited in two ways:

**India and US**
We worked with a professional recruiter to identify interested and qualified candidates for the study. Participant groups for each site were then selected from these pools to create samples representative of the demographics of workers in those occupations in those locations.

**Sub-Saharan Africa**
Participants from the sub-Saharan Africa site work for a company that had developed a set of machine learning applications to assist their employees. This company was interested in better understanding its employees’ perspectives on the new software and the ways it has changed their work. The company facilitated introductions to a group of employees with experience using the software. The group could opt into the research. Participation was entirely voluntary. A strict firewall was implemented from the outset of the research to protect participant confidentiality and ensure they felt comfortable speaking freely about their experiences.

**HOW IS AI AFFECTING INFORMAL WORK?**

Though the primary research in this report is focused on formal sector workers, 60% of the world’s workers participate in the informal sector. While few, if any, work directly with AI systems, AI is still transforming their work by changing informal labor market conditions.

Consider agriculture, where over 90% of the workforce is informal. Globally, informal workers are two times more likely than formal sector workers to be members of the working poor and agricultural workers are more likely than other informal workers to be poor. Many are sharecroppers and contract farmers who make deals with formally incorporated companies to grow specific quantities of specific crops over a given period of time. Historically, negotiations would take into account an informal worker’s accumulated knowledge of local soil and weather conditions, performance of past crops, prior market prices, and other factors. Informal farmers possess the type of experiential knowledge passed through communities and generations, which can be formidably accurate. The companies, on the other hand, possess the type of technocratic knowledge built through the collection and increasingly sophisticated analysis of data.

With the introduction of AI, informal farmers’ ability to negotiate critical provisions has radically decreased. Many farmers now face take-it-or-leave-it offers to produce crops they’ve never seen grown and which may require a year or more of invested cultivation before producing sellable yields. The unprecedented nature of the offers means farmers lack experiential knowledge to base their decisions on, and contracting companies are not sharing the details underlying their proposals, creating sizable information asymmetries.

The experience of the Self Employed Women’s Association (SEWA) in India working with women farmers in the informal sector has revealed a lack of inclusive, quality data. The algorithms used by companies rely on data collected by researchers and economists. Informal sector workers, and in particular women, have not been included in the design of data collection tools or the data collection itself. The exclusion of their perspectives and knowledge raises questions about the usability, authenticity, and relevance of this data.

The contracts created with this data are increasingly non-inclusive, and transfer risks to poor smallholder farmers, pushing them deeper into a vicious circle of poor data representation, poor contracts, high risk, increased poverty, and ever-growing debt. There needs to be a substantial focus on including small and marginal women farmers in the data collection processes, resulting in transparent and inclusive data captured firsthand from informal sector workers.
Major Themes and Findings

The workers participating in this research shared stories, experiences, and observations of their time interacting with AI in their workplaces. The findings of this report are drawn from their insights. While common themes manifested differently according to setting, they appeared across all of the research sites and reflect what we heard from a substantial portion of participating workers. The ways these themes might present themselves (including in settings beyond those we researched) depend on a number of factors, including regulatory protections, companies’ managerial priorities, and workers’ relative influence in their workplaces (through unions, worker organizations, or individual leverage due to local labor market conditions). Workers also experience these impacts unevenly as individuals. Personal demographic characteristics — such as their race, age, gender, immigration status, disability status, and formal education level — may lead them to be more marginalized or vulnerable.

Theme 1: Executive and managerial decisions shape AI’s impacts on workers, for better and worse

Workplace AI is deployed by particular executives and managers in specific contexts and specific ways. Leaders and managers determine whether to use workplace AI technologies, which workplace AI technologies to use, what goals they are intended to accomplish and how they are to be used. These decisions are driven by a combination of business models, company culture, industry trends, and the availability of relevant AI products. These factors also shape each other. The initial choices made by companies that produce technological impacts on their workers are, at first glance, not technology decisions at all: they’re foundational choices about the operating model and personnel strategy of their business.

How hierarchical is the business model? How much discretion are employees given to use their own judgment in executing their work (as opposed to following a strict set of rules and procedures)? Are employees encouraged to stay and develop expertise and experience that they bring to their roles or intentionally churned to keep costs low? Are jobs designed so that they can be performed with very little training (rendering workers intentionally interchangeable) or do they reward experience? How aggressively are performance targets pushed and punished?

These foundational decisions in turn structure subsequent decisions about what technologies could be useful in meeting business goals, as well as how they ought to be used. Upstream decisions on questions like these likely have a significantly higher influence over how AI affects workers than any choices made by their immediate managers.
For instance, a company that designs a “high road” model and strategy to offer its workers high degrees of autonomy (a job attribute highly correlated with high job quality and employee satisfaction\textsuperscript{54}) would likely see more value in non-binding AI decision-support tools. On the other hand, a company that designs a “low road” model, with its roles to be performed with very little training or autonomy and very short average tenure (highly correlated with low job quality and employee satisfaction\textsuperscript{55}) would see more use in technologies that closely monitor work to ensure it is being performed correctly or claim to remove the need for human judgment. Each of these decisions has an impact on workers, shaping what tasks they are expected to accomplish and how they are expected to do them. All of these decisions impact workers beyond technology, potentially much more than any technologies used — but they also shape workplace AI’s impacts.

As an example, the customer service agents we spoke to in India use AI software marketed to customer support companies and teams as real-time coaching, performance assessment, and task augmentation for their agents. One function of the software is to monitor their calls and text chats for keywords and phrases to diagnose possible customer issues and suggest resolutions, which are offered to agents in real-time pop-ups and menus. Another function is to monitor tone of voice, volume, and keywords to assess emotion and offer real-time pop-ups and alerts to agents on how they could better manage the emotional side of their interactions with customers (for instance, warnings that conversations are sounding emotionally charged, or guidance to speak more quietly, or slow down their speaking speed).

In the agents’ use of this software, two clear examples of this theme emerged. First, for some agents, it was clear from their employers’ guidance that they should take AI alerts and prompts they received during calls or text chat sessions as suggestions, rather than commands or requirements. This group of workers was expected to exercise autonomy and judgment in meeting customer needs, using the AI feedback as one of many inputs in their call or chat handling. Agents at different companies were expected to closely follow the feedback from the AI and not disregard its recommendations except, perhaps, in extreme circumstances. Both groups recounted instances where they judged the AI to be incorrect in its recommendations, but the group empowered to deploy their judgment on calls or in chats felt more autonomy and control over the quality of the service they provided. Some employers treated AI feedback and call assessment (including predictions of customer feedback scores) as purely a coaching tool. Others used it as a direct input to performance evaluations. In a coaching setting, workers were able to put the feedback in context for themselves, adopting suggestions where they made sense. In a performance evaluation setting, the context was often flattened or missing, adding an element of arbitrariness where managers likely intended to add rigor.\textsuperscript{56}
In sub-Saharan Africa, the data annotators were tasked with annotating images or videos for data sets to be used in developing machine learning (ML) models. Prior to the introduction of machine learning software to automate part of this work, the workers carefully outlined each contour of an object in an image. For videos, this could require them to meticulously shift the position and edit the contours of the outline for dozens or even hundreds of frames where the object had only slightly changed position from one frame to the next. The company recently introduced ML task automation software to assist the workers in the fulfillment of their roles. For certain objects in an image, workers could identify the outermost corners of the object and the software filled in the rest. For videos, the software could take the initial object outline delineated by the worker and predict the outlines of that object in many future frames.

The workers who participated in this research were tasked with testing and providing feedback on the company’s new ML software (in addition to being responsible for actual annotation work). Unlike other workers responsible for specific client deliverables and deadlines, they were not given strict quality or completion performance targets for the annotation side of their role. They still, however, had the opportunity to earn bonuses for the speed and accuracy of their work. This incentive structure for their work gave them the needed time and freedom to focus and reflect on improvements to the ML tools that could deliver value for the company without forcing them to miss out on the opportunities for additional compensation offered to their colleagues.

Previous research has offered other demonstrations of how managerial decision-making shapes AI technology’s impacts on workers. This includes the use of big data analytics as invasive and harmful “bossware,” the cruelty that can result from algorithmic decisions with no human recourse, the negative health impacts of overly aggressive performance targets set using AI, the lack of worker protections afforded to workers misclassified by their employers as independent contractors on AI-driven platforms, and the negative health impacts, life disruptions, anxiety, and job insecurity arising from last minute shift-scheduling enabled by AI software.

These negative impacts on workers should not be seen as inevitabilities of the unstoppable march of technological progress, but rather as the outcomes of a series of decisions. These decisions are made first by companies who create business and operating models revolving around low-quality jobs, then by product developers and designers who build AI technologies that are either explicitly designed for these uses or possible to misuse in harmful ways, and subsequently by leaders and managers who choose these particular implementations. The beneficial examples above, where AI software was used to assist workers while they maintained their autonomy and retained decision-making authority, demonstrate that better choices are available for managers and leaders implementing AI in their workplaces.
Workers appreciate how some uses of AI have positively changed their jobs

While there are clear harms arising from some workplace AI uses and decisions, the role of workplace AI in job quality is not wholly negative. Across our research sites, workers offered reflections on what they appreciated about specific uses of AI or attributes of AI products that they use. In the India site, in addition to the appreciation for additional information to support their decisions, and real-time coaching that was not evaluative or punitive, workers highlighted time-saving as well as benefits to their physical well-being from AI software that logged caller details and auto-prompted solution menus. The call center workers also reported that the software’s automated data entry reduced eye strain and repetitive stress injuries to their wrists and hands compared to the constant keyboard, mouse, and screen work needed when entering this information themselves.

In the sub-Saharan Africa site, a strong majority of the data annotators preferred working with the ML tools compared to when they did their work more manually. They lauded the speed with which the ML prediction software enabled them to complete annotation tasks, and the reduction in sometimes tedious or boring repetitive work. (For instance, working their way through each frame in a video from start to finish.) Some workers also mentioned that the tool helped them feel less tired throughout the day or at the end of their shifts. However, they noted the software also sometimes had accuracy problems. In these cases, many workers would have preferred to manually complete those tasks themselves from start to finish. When the software was inaccurate in its outputs, it posed several problems to the workers. First, it forced them to use their time inefficiently — not only did they have to spend the time waiting for the algorithm to complete its (incorrect) annotation, they also had to spend additional time revising the output from the software. Second, the process of trying to find each error and then correct it felt unnatural and painstaking compared to when they felt mentally prepared to just do the tasks themselves. Finally, they felt a sense of frustration familiar to anyone required to work with a malfunctioning technology: the software was failing to meet their expectations and leaving them to sort out the problems it created. In interviews, the data annotators explained that part of this performance gap could be attributed to portrayals of the technology when it was introduced. Because it was “machine learning” or “artificial intelligence,” they expected it to be more accurate than their own work, not less. Still, even workers who expressed these issues praised the benefits listed above when the technology was working properly.

While there is a broader, ongoing discussion of puffery in the AI industry, less coverage has been afforded to the effects of similar dynamics in workplaces. Inflated portrayals of workplace AI’s capabilities may do more harm than good. Setting high expectations (however inadvertently) and then failing to meet them was a source of frustration and stress expressed by the call center workers regarding the call-coaching and evaluation.
software as well. In the context of AI’s benefits to workers, setting realistic expectations and then meeting or exceeding them may substantially reduce friction in AI use.

Among the warehouse workers in the US, many singled out AI technologies that reduced possible errors, such as placing items in the wrong locations or using the wrong tape or labels on packages. A number of participants said they felt an increased degree of pride in their job due to their accuracy in their work. Some research participants additionally valued how warehouse robots reduced some physical demands of the job. In the case of robots that bring items to workers, this could be a radical reduction in steps walked by workers who previously would have walked 10 or 20 miles a day to get these items themselves. The assistance of robotic arms could reduce muscle strains and pulls. Positive reactions to these physical effects were mixed, however, with some participants noting that they missed the exercise they got in the old way of working and others raising concerns about increases in injuries from repetitive movements prompted by the robot-assisted workflow.69 70 71

Some of these benefits of workplace AI commonly cited by workers — like increases in speed, accuracy, efficiency, and productivity — were clearly intended by the creators and implementers of the technology. Others, such as the sense of pride in a job well done, could be seen as indirect effects of those benefits intentionally sought by the AI creators and implementers. Still others, such as the ergonomic advantages of automated call-logging, were meaningful improvements to worker well-being that likely did not play a decisive role in the creation of the software or the company’s decision to purchase it, but accrued to the worker nonetheless.

Both the intended and unintended positive consequences of workplace AI cited by workers point towards possible paths for developing and implementing workplace AI technologies that benefit workers as well as their employers. The workers who spoke with us and shared their stories and experiences were not anti-technology or anti-AI. Their own descriptions of what counts as a good work day and their personal definitions of what it means to do good work share a number of values and goals with their employers, including swift and accurate completion of their tasks. The participating workers welcomed technological assistance in achieving these objectives, provided they could maintain or improve their job quality while using it. The positive experiences of AI and perspectives shared by workers should give businesses confidence that benefits to workers and benefits to employers are not zero-sum. Workplace AI integrations can deliver value to both groups. Respectful, considered AI implementations that maintain worker dignity and autonomy can be embraced by workers.
While AI may be relatively new to most workplaces, the impacts workers see from its use are not. Many negative impacts from workplace AI are versions of impacts seen from non-AI technologies. For instance, employers may make job and task design decisions encouraging repetitive motions that could lead to injuries (as reported by some participating warehouse workers) in order to integrate AI task automation into workflows. This also occurs in other, non-AI assisted industrial settings where workers are assigned a small set of tasks to perform repeatedly. AI systems can deliver negative feedback to workers without helpful suggestions for improvement: an issue noted by some participating customer service agents and also an unfortunate practice of some human managers since the creation of managerial and supervisory roles. Additionally, some companies deployed intensive monitoring of their workers well before big data and AI made it possible for managers to analyze that data in increasingly invasive and stressful ways.

A US warehouse worker offered a representative explanation of how a performance evaluation AI system layered into her job — a monitoring software used by her company to provide real-time performance feedback — negatively affected her emotional well-being. From when she clocks in until she clocks out, she is constantly monitored by software. The software tracks when she is completing a task (for instance, following instructions she has been given about how to process an item in the warehouse). It tracks how long it takes her to complete that task, tracks when she is between tasks, tracks when she goes to get water or use the bathroom. And it tells her whether she is staying on pace or falling behind the goals her company managers use that same data to set. The expectation is that she is constantly on pace. If she falls behind for any reason, it triggers stress that stays with her until she is ahead of the targets again. The stress isn’t from personal perfectionism: firing is a common consequence for workers who fall behind targets at her employer, regardless of whether they might have understandable reasons for a slower pace (for instance, health conditions that might require more frequent breaks).

The pressure generated by the way her company management uses this software leads her and her colleagues to cut corners to speed up their work. When they’re trying to stay on pace, she and some of the other warehouse workers pointed out that they would sacrifice safe or proper movements or lifting techniques in favor of speed. The consequences their employers set for being too slow made the choice clear for them: they focused on not getting fired over making sure they stayed safe. While some technologies in AI-assisted warehouses can reduce physical burdens on workers, such as robotic item movers which reduce the distances workers walk in a shift, employers’ decisions to use AI technologies to accelerate the pace of work can create higher worker injury rates.\textsuperscript{72, 73}
On top of the emotional and physical well-being issues that workplace AI can cause, the way managers and executives choose to integrate AI into the overall workflow may lead to lowered intellectual well-being on the job. Workers at each site largely agreed that the AI systems used in their jobs lowered the level of intellectual challenge when compared to what it looked like to do their work without AI. Workers in US warehouses with higher degrees of AI implementation often had less variety in their tasks and more technological guardrails to assist them in performing them correctly. The customer service agents in India spent less time and energy diagnosing the reasons a customer called or identifying possible solutions for their issues. In sub-Saharan Africa, the data annotators no longer completed intricate tasks requiring a careful, discerning eye from start to finish, but instead largely spent their time creating broad outlines around objects in images, letting algorithms do the rest. While many welcomed the extra ease, many others indicated that they preferred a higher degree of challenge.

Each of the examples offered above can be seen as a continuation of trends from other workplace technologies. However, existing laws and regulations do not appropriately address these harms. The status quo enforcement of basic health and safety protections for workers around the world is inadequate to prevent them from being harmed by their jobs: the introduction of AI software and systems that can ratchet up work intensity only increases the urgency of shoring up these laws and their enforcement. In addition to the emotional and mental health impacts described above, AI monitoring and surveillance technologies undermine workers’ sense of privacy, dignity, and autonomy. Yet mental health safeguards are often less regulated or enforced and a policy vacuum exists in many geographies regarding privacy and data protections at work.

The familiarity and continuity of harms from workplace AI should make them easier to anticipate, and thus to prevent or mitigate through responsible design and use. But until consideration of these impacts is foregrounded by AI developers and the executives and managers who purchase and implement workplace AI, or sufficient protections and enforcement are enacted by governments, workers will continue to suffer harms that could have been anticipated and prevented.
Current implementations of AI in work are reducing workers’ opportunities for autonomy, judgment, empathy, and creativity

One optimistic line of thought on AI’s transformational effects on jobs suggests AI will support humanity to take on more creative, empathetic, or intellectually advanced work⁷⁶,⁷⁷—an admirable goal of creating jobs with more “human” tasks than the reproducible, mathematically definable work of algorithms and robots. As reported by workers collaborating closely with AI, however, the current reality on the ground points to jobs moving in the opposite direction.⁷⁸

Take the data annotators working with an ML technology that automates some of the annotation work they would have previously done manually. Their responsibilities shifted away from a creative, generative role that some of them described as like a craft or art. Previously, they carefully drew the outlines of relevant objects and derived satisfaction from their precise handiwork. With the addition of ML software to their workflow, they now, in their words, spend less time creating and more time “fixing” or “cleaning” the AI’s output by identifying and editing images that the algorithms annotated incorrectly.

Some of the call center workers used technologies designed to address two of these supposedly more human skills: empathy and problem-solving. For empathy, call monitoring software assessed whether calls were getting too emotionally charged by measuring agents’ volume, speed, and word choice. For problem-solving, a software designed to assist agents detected keywords and phrases in order to pull up solution lists and suggest possible issues the customer or client might be having. In each case, the software was not consistently accurate or helpful (according to the judgment of the experienced call center workers) but workers often had to contend with performance assessments tied to complying with this software by making their displays of empathy more templatized and, ultimately, less human.

In automated warehouses, workers who had been around prior to the introduction of new AI and robotics systems, or who switched from warehouses with less automation to cutting-edge robotics locations, found that the variety of their tasks shrank over time, with AI, robotics, and other automated systems picking up tasks that they previously completed or coordinated with other workers to complete. Multiple workers mentioned feeling like they themselves were also robots in the more automated warehouses. Along with workers’ increasingly parochial view of the work being done throughout the warehouse came a decrease in their positioning and ability to identify and suggest improvements at a systemic level. Their universe of problem-solving potential had shrunk from warehouses sometimes the size of seven New York City blocks to a small set of tasks at a workstation no greater than 10 feet by 10 feet.

Each of these examples points to an under-discussed and heterodox aspect of current uses
of AI on job quality and skills: current managerial decisions and technological products mean the transition to the purportedly attainable full automation of a specific job could well be one where the workers in that job experience less autonomy (and thus fewer opportunities for creativity, empathy, complex problem-solving, and judgment), not more.

These “transition to automation” periods can be extremely long, as incremental progress either continues or stalls and researchers work for the next breakthrough. See, for example, the delays relative to predicted timelines for self-driving cars.\textsuperscript{79} When thinking about workers training their AI replacements, some may have in mind the time horizon of training another human to do your job — but these periods of automation transition could last years, decades, or possibly the span of an entire career.

Depending on how the technology evolves, workers may never see a paradise of creativity on the other side. This is perhaps a corollary to, or a deepening of, the “paradox of automation’s last mile” suggested by Mary Gray and Siddarth Suri in \textit{Ghost Work}.\textsuperscript{80} While their work highlighted the possibility that there will always be more work for humans in the quest for full automation, workers’ present experience working with AI systems tells us a great deal about what it will look like for many workers to traverse that paradoxical last mile.

This is an issue that comes through more clearly in light of the distribution of skills and tasks throughout the labor market and the ways managers and companies decide to combine human and AI labor. In jobs where companies are actively trying to automate some or all of the tasks, they need workers to produce training data: both for originally building the relevant algorithms and for continuous improvement. The current state of AI chasing the replication of human abilities means automation technologies are largely focused on discrete, narrow tasks — and so, too, are the workers tasked with training them.\textsuperscript{81} Given these structural forces, it’s not surprising that the ways these AI technologies are deployed reduce workers’ scope for exercising these more “human” tasks in their jobs.

The realities of how current managerial uses of AI technologies transform workers’ jobs suggest a need to re-evaluate the optimistic framing in multiple ways. To the extent that executives and managers see value in using AI technology to free up their workers to perform more “human” or advanced tasks, they cannot assume that any AI tool will meet that goal. Nor should developers take for granted that the AI tools they create, as implemented, will free up humans to be more creative or empathetic or to focus on tasks requiring more complex judgment or discernment. Without caution and active collaboration with workers, these workplace AI product adoptions may bring about the very opposite effects. Moreover, the uneven pace of AI development means that these current impacts ought not be brushed aside as temporary harms on a quick path to a better future. The future capabilities of these technologies remain unclear, as do the timelines to achieve them.\textsuperscript{82} The present-day harms to existing workers’ autonomy, dignity, and senses of satisfying and meaningful work, on the other hand, are real — and accelerating.
Empowering workers early in AI development and implementation increases opportunities to implement AI that benefits workers as well as their employers

The market for workplace AI products is presently structured to address needs and opportunities perceived by company leaders and managers with substantial budgets for AI transformations or integrations. Workers who use these products are multiple layers removed from decision-makers and may also be in different departments or reporting lines. As such, the priorities of AI purchasers are not necessarily those of workers.

Providing workers the opportunity to participate in the creation, design, and implementation of workplace AI is a necessary corrective to approaches that exclude workers only to later require them to use technologies created without their input or the centering of their needs. Not every worker who participated in the research wants these opportunities for input. But comprehensively excluding this group throughout the process or until UX (user experience) or user-testing phases has multiple negative effects.

The data annotators who participated in this research were tasked with helping to improve the ML software they used in their work. They described their team leaders and the developers they worked with as open to suggestions, and they took pride in troubleshooting, bug-spotting, and identifying improvements to the software that were later adopted. Interviewees thought their ideas and suggestions meaningfully improved the tools they worked with. Even in this intentionally participatory environment, however, their reflections revealed some missed opportunities. In broad strokes, they described their role as finding ways to improve the software’s effectiveness. Nested underneath this mission were implicit objectives like understanding the nuances of the software’s failure modes or identifying improvements for the user interface. Since the software was useful but frustrating when it failed, improvements to its effectiveness also contributed to their own satisfaction.

However, they appeared to consider participation in shaping other aspects of their work or offering ideas for new technologies as outside their responsibilities. Recall, for example, the workers who found it disruptive to their efficiency and flow when the ML software struggled and they had to edit its mistakes. An annotator offered the idea of giving annotators the ability to set those images aside to return to later, allowing them to process all of the successful automations in one batch, and all the tasks requiring their edits in another, rather than bouncing back and forth without a sense of what the next task would require. The suggestion was a process improvement that could improve worker satisfaction and likely task efficiency. When asked in a follow-up question whether the annotator had made that suggestion to their managers or the developers, they responded that their job was to improve the effectiveness of the tool, not ideas like this.

By not opening up the biggest possible spaces for worker participation, or not asking the right questions, designers and implementers are missing productive ideas for new
technologies. What would a worker in this role identify as the biggest issues they’d like tech to help them solve or tasks they’d like assistance with? How could workflows, jobs, and business processes be reimagined for the better from workers’ perspectives? What would a welcome technological aid or solution look like from their perspective?

A number of the participating customer service agents, for instance, flagged angry customers as one of the worst parts of their jobs. They had no advance notice of whether their next interaction would be with someone who would be respectful or abusive to them about mistakes by their employer, and which were out of their control. When asked if there were areas where they would welcome AI in their jobs, multiple agents suggested de-escalation technologies, or warning systems so they at least knew what they’d be facing — both of which agents were confident would improve customer experience as well.

Without worker participation from the start, AI developers also lack important information about design and use. What common or uncommon occurrences in the workplace would cause this technology to fail or struggle? What does every experienced worker in this role know that outsiders would find difficult to identify or understand? Moreover, workers left out of the process may be less inclined to trust or adopt AI tools.83 In an alternative world where workers were included from the start, how much more effective could a given technology be? How much more quickly could it be launched at scale?

Not having the workers who will use the technology “in the room” means that projects get greenlit and products get designs that are, on the whole, not worker-centric. Worker-centricity is one of many possible goals for a product team. Without consistent, empowered advocates for that goal present, it is structurally probable to be deprioritized relative to priorities of senior leaders, designers, and engineers.84

Many workplace AI systems (including several described in this research) also reflect and reinforce a managerial mindset (perhaps best described as “neo-Fordism” or “neo-Taylorism”) where deskilling and strict control over workers is seen as the path to the highest profitability. The origins and drivers of this approach in AI development has not been accounted for in detail (for instance, did limits to AI capabilities shape this approach to workplace AI products, or did strong belief in this managerial approach shape a market that AI developers then filled?), but the impact on workers remains the same — they are treated as subjects in need of discipline and control, rather than as professionals with valuable expertise.

Alternative management approaches used in sectors as varied as manufacturing85 and hospitality86 encourage frontline workers to draw on their accumulated expertise and judgment to address problems and make improvements. These approaches afford workers the needed influence and decision rights to make their recommendations stick.87,88 Treating workers as genuine experts and empowering them to participate in AI development and deployment offers opportunities for both workers and businesses to benefit.89
Opportunities for Impact

Actors across the AI investment, creation, deployment, use, and regulation spectrum have opportunities to make decisions that center workers’ voices and protect their well-being. As shown above, the benefits of these decisions do not need to be zero-sum: there are paths forward that can benefit both workers and their employers. Specific recommendations and opportunities for impact are outlined by stakeholder group below. While the recommendations are structured by the audience most able to take action on it, change and accountability also rely on the relationships between different actors (for instance, the complicated ways in which the actions of both AI creators and AI implementers drive the workplace AI products available for purchase). In practice, these interactions may have allowed some decision-makers to evade culpability for their actions; accordingly, these relationships and dynamics should also be considered in the implementation of these recommendations. In the event that actors are attempting to avoid responsibility for harms or negative effects, others must take care to hold them to account.

The benefits of these decisions do not need to be zero-sum: there are paths forward that can benefit both workers and their employers.
Employers that choose to use AI in the workplace have an obligation to ensure it does not decrease their employees’ well-being. They also have the highest degree of control in ensuring this outcome. employers might not directly create the AI-enabled workplace products on the market, they can choose which products to use (or choose to use none at all) and set the contexts and conditions for their use. Employers determine when AI is used (e.g., in core or non-core tasks) and how (e.g., as a decision-support tool with a human worker given the ultimate say or as a final decision-making tool). As shown above, this set of decisions has profound influence over how workers experience workplace AI, even in cases where employers are using similar AI products.

### OPPORTUNITIES FOR IMPACT

<table>
<thead>
<tr>
<th>Values and governance</th>
<th>Commit to making worker-centric/worker-friendly AI that increases access to better jobs, especially for the most vulnerable and marginalized workers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AI product purchasing</strong></td>
<td>Take workers and their institutionalized representatives seriously as experts in their own roles and incorporate their input into purchasing decisions, including:</td>
</tr>
<tr>
<td></td>
<td>• Which problems and opportunities to seek AI solutions for. (For instance, seeking technology to support workers in their roles in ways that they have identified rather than the current focus on punitive surveillance tools.)</td>
</tr>
<tr>
<td></td>
<td>• Which solutions to select out of an AI product category.</td>
</tr>
<tr>
<td><strong>AI product implementation</strong></td>
<td>Integrate frontline workers and other end-users’ perspectives into the implementation of AI (e.g., workflow and performance targets).</td>
</tr>
<tr>
<td></td>
<td>Give humans working directly with AI systems the final judgment on AI-supported decisions, especially in situations where they could affect workers’ performance evaluations and lives outside of work.</td>
</tr>
<tr>
<td></td>
<td>Foster and seek out representation from institutionalized forms of worker organization, ensuring that workers can offer their authentic views without fear of retribution or retaliation.</td>
</tr>
</tbody>
</table>
Core technologies underlying workplace AI tools are created by an increasingly concentrated group of companies. This concentrated group may use them internally and also sell these technologies to other businesses. Values and practices that center the participation and well-being of worker end-users at these companies have the potential for transformative changes in job quality around the globe. These values and practices are all the more important in the market for workplace AI products, one where company leaders and managers are purchasers and the users may be some of the lowest paid and least influential or powerful employees in the company. This market structure means a focus on customers is not necessarily a focus on worker end-users (and vice versa).

These divergences are likely particularly pronounced in companies with strong command and control approaches to integrating AI into their workplaces as outlined above. Not coincidentally, these companies often employ large pools of low-wage workers most vulnerable to AI’s negative effects. Creating better feedback loops and genuinely centering workers will often require seeking out the participation of workers and their representatives beyond their own organizations. There are, however, areas of alignment between the needs and preferences of workers and the incentives of business leaders and managers (as discussed in more detail in Theme 3). While not all of the applications sought by company leaders and managers may be endorsed by their workers, focusing on the overlap adds an additional constituency in support of particular products: the workers/end-users.

### OPPORTUNITIES FOR IMPACT

**Values and governance**

Commit to making worker-centric/worker-friendly AI that increases access to better jobs — especially for the most vulnerable and marginalized workers — by measuring workplace AI products’ impacts on job availability, wages, and job quality, and working to eliminate or mitigate negative impacts.

Include workers as participants and key stakeholders in creating any company’s AI ethics/responsible AI principles.

Recruit staff of diverse backgrounds to AI development teams and actively work to retain them as staff after recruitment. While representation on its own is not a solution, the relative lack of diversity in AI product teams can contribute to the creation of blindspots that could be mitigated by more diverse teams.

---
Incorporate workers and other end-users’ perspectives from the beginning of the product origination process. That is, work forward from problems, challenges, and opportunities identified by frontline and other workers toward products rather than finding ways to shoehorn research progress into workplace products and routines. Collaborate with workers’ institutionalized representatives where possible.

“Red-team” potential use of workplace AI products from origination through major update cycles. Without intentional focus, developer and product teams may not identify the potential for misuse or harm. Eliminate or mitigate identified opportunities for uses harmful to workers, especially in situations where technologies may be sold and deployed in contexts with fewer worker protections than they are developed. Responsible red-teaming and harm mitigation may require companies to not pursue product ideas where harms cannot be mitigated. Particular attention must be paid to the diversity and heterogeneity of use contexts, including ones where potential dimensions of marginalization and inequality (e.g., gender, class, age, ethnicity, race, religion, sexuality, disability status) may not be the same as the cultural and social context of the developing company or team and where existing power imbalances limit the opportunities to reject, restrict, or limit use.

Collaborate with workers to identify areas where they would welcome assistance in completing their work with augmenting AI or automation of non-core tasks, drawing upon the complementarity of humans and AI.

Foster and seek out institutionalized representation of workers, ensuring that workers can offer their authentic views without fear of retribution or retaliation.

When seeking to include the perspectives of workers, recognize that workers from different backgrounds and of different demographic categories may experience workplaces and AI technologies in different ways. Seek broad, representative participation and feedback, and work to ensure workers of all backgrounds feel comfortable and empowered when participating.

Take workers seriously as experts in their own roles and include them in product development and future update cycles. Create opportunities for their empowered participation as subject matter experts, not just as end-user testers.
Workers and the organizations and unions that represent them can shape AI’s impacts on their workplaces through contract negotiations and other mechanisms to influence corporate policy as well as on-going input into purchase and implementation decisions. Unfortunately, it is not common in many countries for employers to invite this participation and the ways AI technology shapes job quality and worker well-being can be obscured. Education and training programs by unions and worker organizations can help workers understand the functions and roles played by AI products and equip workers to participate in decisions made to purchase and implement AI in their workplaces.

**OPPORTUNITIES FOR IMPACT**

<table>
<thead>
<tr>
<th>Unions and worker organizations</th>
<th>Foreground worker voice in development and implementation of AI (and other technology) as a plank of contract negotiations and other mechanisms to influence corporate policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Train members and organizers in relevant technologies and their benefits and drawbacks, spotlighting AI technology and related issues (e.g., data rights) as a major influence on working environments.</td>
</tr>
<tr>
<td>Workers</td>
<td>Actively seek to participate in workplace AI purchasing and implementation decisions.</td>
</tr>
<tr>
<td></td>
<td>Ask for disclosure and transparency on technologies being used, data being collected, how it’s being used, and for what purpose.</td>
</tr>
<tr>
<td></td>
<td>In workplaces with cultures of including workers in management decisions, offer input on areas where AI technology solutions would be welcomed and suggestions about ideal implementation.</td>
</tr>
<tr>
<td></td>
<td>Seek out worker organizations and unions operating in the same sector and geography undertaking efforts on these issues.</td>
</tr>
</tbody>
</table>
Through laws and regulations concerning both technology and labor, government lawmakers and regulators shape the environments in which AI products are developed, sold, and implemented, and thus shape the technologies themselves. As discussed above, there are and will continue to be instances where the incentives of AI-creating and -implementing companies strongly diverge from the interests of their workers. In such instances, government action will be required to ensure the livelihood and well-being of workers; as the historical record indicates, few businesses will voluntarily shoulder the whole of these changes. Compounding this, lack of worker voice and power often comes down to lack of worker protection (e.g., for organizing or ensuring correct worker classification). In some cases, AI technology further enables employers to exploit these power imbalances and policy or enforcement gaps. Strong regulation and enforcement, including of existing laws and policies, is all the more critical in these situations.

The heavily concentrated nature of the global AI research and workplace product development industry means that many workplace AI technologies are developed in and sold from the United States and China and then implemented in other regulatory environments. While the fractured, global nature of AI’s impacts on workers impedes concerted efforts to protect workers, divergent regulatory environments offer opportunities for the experimentation and sharing of best practices in line with local norms and values. Conversely, countries with less economic power or enforcement capacity may find themselves in the position of reacting to harmful technologies created at or implemented from a distance; these situations require careful consideration and differentiated responses.

Much of the African continent, for instance, is both less well-placed to reap the economic benefits of AI (due to a comparative lack of telecom, computing, and other infrastructure, as well as a comparatively small skilled AI workforce), and more susceptible to potential workplace and labor market harms from AI use inside and outside the region (due to a comparative absence of protective regulations targeting AI use and impacts and weaker enforcement capabilities for labor protections). While a number of countries have been making recent strides on these factors, they are beginning from less advantageous starting points and starting at later dates than many high-income countries and regions. Proactively investing in AI workforce development and supporting infrastructure opens up the possibility of more “home grown” solutions responsive to local needs and values, rather than the status quo importation of technology from abroad that may undercut local social goals.
<table>
<thead>
<tr>
<th><strong>OPPORTUNITIES FOR IMPACT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Worker voice</strong></td>
</tr>
<tr>
<td><strong>Worker protection</strong></td>
</tr>
<tr>
<td><strong>Tax policy</strong></td>
</tr>
<tr>
<td><strong>Investment regulation</strong></td>
</tr>
<tr>
<td><strong>Research grants and proposals</strong></td>
</tr>
<tr>
<td><strong>Low- and middle-income country (LMIC) responses</strong></td>
</tr>
</tbody>
</table>
Private investment in AI technologies doubled between 2020 and 2021, directing ever higher amounts to a concentrated group of companies.\textsuperscript{113} While angel and venture capital funders have not traditionally focused on the ESG (Environmental, Social, and Governance) impacts of their investments, the push for higher investor responsibility for climate change and sustainability impacts marks a shift in this attitude. Large institutional investors, similarly, are beginning to articulate an investment thesis of “stakeholder capitalism”\textsuperscript{114} inclusive of companies’ treatment of workers.\textsuperscript{115} In the United States, the Securities and Exchange Commission (SEC), which is responsible for regulating government investments, has proposed additional workforce disclosures related to treatment of workers, arguing that they are material information for investors.\textsuperscript{116} As AI is increasingly adopted by companies, investors can influence its path by understanding and accounting for the downside risks posed by practices harmful to workers and the potential value created by worker-friendly technologies and practices.

**OPPORTUNITIES FOR IMPACT**

<table>
<thead>
<tr>
<th>Investors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Include job availability and quality impacts of AI technology in ESG impact measurements for AI-creating and AI-implementing companies.</td>
<td></td>
</tr>
<tr>
<td>Offer and support shareholder proposals to increase workers’ voice and well-being.\textsuperscript{117}</td>
<td></td>
</tr>
<tr>
<td>Request anticipated impact on workers when evaluating proposals and pitches for workplace AI products and companies.</td>
<td></td>
</tr>
<tr>
<td>Work with institutionalized forms of worker representation in order to solicit authentic, unencumbered perspectives of workers to incorporate into ESG metrics, stakeholder capitalism initiatives, and other efforts intended to increase worker well-being.</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

Current uses of AI and its existing technological path pose significant risks to job quality and worker well-being. Future research is needed to better understand the impacts of AI on informal workers, as well as to quantify the business case for and possible tradeoffs of the recommendations in this report. However, opportunities exist for developers, employers, workers and their institutional organizations, governments, and investors to correct the course, steering AI in a direction that benefits workers as well as their employers.

The Partnership on AI is leading an effort — in continued collaboration with workers at the frontier of AI implementation — to develop commitments and targets for AI's impacts on job quality as well as tools to support stakeholders in implementing these targets and commitments. To learn more about this effort and stay updated on our work, visit the AI and Shared Prosperity Initiative page on PAI's website.

The ways AI degrades job quality and worker well-being in the present are neither inherent to the technology nor inevitable outcomes of its progress. Stakeholders have the power to transform AI’s trajectory for the better. It is incumbent upon them to use it.
Acknowledgments

This research is based on the reflections and comments of nearly 80 workers in India, sub-Saharan Africa, and the United States who work with AI every day in their jobs. Without the insights and stories they shared in the diary study and their interviews, this research would not have been possible. We thank them for sharing their time and expertise with us.

We appreciate the employees of the company who took an interest in the goals of this research and supported its execution by introducing us to their colleagues whose participation formed the sub-Saharan Africa site, as well as the professional firm which assisted us with recruiting participants at the India and United States sites. Each of them went above and beyond to ensure we were able to connect with people directly experiencing AI’s complex effects in their workplaces.

The members of the Steering Committee for Partnership on AI’s AI and Shared Prosperity Initiative shared their expertise and feedback on this research throughout the scoping, design, analysis, and writing process. Their astute contributions and detailed comments on earlier drafts have strengthened this work immensely. We are grateful for their guidance. We additionally appreciate Mary L. Gray for taking the time to share her valuable suggestions on early versions of our research questions.

We would also like to thank the Partnership on AI staff who championed this work and provided thoughtful feedback and ideas throughout the research and writing process: Andrea Cross, Christine Custis, Rebecca Finlay, Hudson Hongo, Sonam Jindal, Katya Klinova, Tina Park, and Neil Uhl.

Finally, we would like to thank the Ford Foundation, and the stewardship of Ritse Erumi in particular, as a generous funder of Partnership on AI’s AI and Shared Prosperity Initiative and of this research.
The AI and Shared Prosperity Initiative Steering Committee

Daron Acemoglu
Institute Professor of Economics at the Massachusetts Institute of Technology

Dunstan Allison-Hope
Vice President at Business for Social Responsibility

Juana Catalina Becerra Sandoval
Visiting Scholar, Responsible & Inclusive Tech at IBM

Michael Chui
Partner at the McKinsey Global Institute

Jack Clark
Co-chair of the AI Index and former Policy Director at OpenAI

Andrea Dehlendorf
Executive Director at United for Respect

Arturo Franco
Vice President for Insight at the Mastercard Center for Inclusive Growth

Jessica Fulton
Vice President at the Joint Center for Political and Economic Studies

Ryan Gerety
Senior Advisor at United for Respect

Stacey MacGrath Gifford
Research Staff Member—Future of Climate, Governance of Science and Technology at IBM Research

Deborah Greenfield
Independent Labor Consultant and Former Deputy Director-General for Policy, International Labour Organization

Anton Korinek
Professor of Economics at the University of Virginia

Andrew Kortina
Co-founder of Fin Analytics and Venmo

Jody Medich
Principal Design Researcher, Office of the CTO at Microsoft and Founder of Superhuman-X

Sabelo Mhlambi
Founder at Bantucracy

Pamela Mishkin
Policy Staff Member at OpenAI

Shakir Mohamed
Senior Staff Scientist at DeepMind

Paloma Muñoz Quick
Advisor at the UN Working Group on Business and Human Rights and OHCHR B-Tech

Grace Mutung’u
Research Fellow at the Centre for Intellectual Property and Information Technology at Strathmore University

Lama Nachman
Intel Fellow & Director of Anticipatory Computing Lab

Reema Nanavati
Executive Director of the Self Employed Women’s Association

Aiha Nguyen
Program Director, Labor Futures Initiative at Data & Society

Rahul Panicker
Principal Technologist and Advisor to the CTO at Vicarious

Damon Silvers
Policy Director and Special Counsel at AFL-CIO

Sarah Treuhaft
Vice President of Research at PolicyLink
Appendices
APPENDIX 1

Detailed Site and Technology Descriptions

OVERALL

FIG. 3 Participant demographics & characteristics: Overall

<table>
<thead>
<tr>
<th>Number of participants</th>
<th>78 Diary studies</th>
<th>47 Interview participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under 35</td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td>35-64</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Union membership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Members</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education level completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary school/</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>High school/GED</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trade school/Associate's</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Post-secondary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>College/University/</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>Bachelor's degree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graduate degree</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Options for gender identification at each site included “Non-binary,” “Other (specify)” and “Prefer not to answer.” None of the participants chose these options.

FIG. 4 AI technology types included in study by worker journey stage and site

<table>
<thead>
<tr>
<th>Employee Journey Stage</th>
<th>Technology Type</th>
<th>India</th>
<th>Sub-Saharan Africa</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROLE FULFILLMENT</td>
<td>Task augmentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Task automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real-time task assignment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COACHING</td>
<td>Real-time performance feedback</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance predictions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Improvement guidance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PERFORMANCE EVALUATION</td>
<td>Performance target setting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## INDIA

<table>
<thead>
<tr>
<th>ROLE FULFILLMENT</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>augmentation</td>
<td>Software that analyzed text-based customer service chats to provide agent with a small set of potential response and resolution templates to use as responses to customer comments</td>
</tr>
<tr>
<td></td>
<td>automation</td>
<td>Chatbot that handled straightforward customer inquiries, automating requests that previously would have been handled by workers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software that captured and logged customer and call details, which previously agents needed to enter themselves</td>
</tr>
</tbody>
</table>

| COACHING | Real-time performance feedback | Software that monitored calls for keywords, key phrases, and tone, and provided pop-up coaching to the call agent in the moment on what to do differently (e.g., greet the customer according to the script; speak more loudly, quietly, slowly, quickly; end the call by a certain time) |
|          |            | Software that monitored calls and predicted customer satisfaction scores |

| PERFORMANCE ASSESSMENT | Performance evaluation | Software that monitored calls and predicted customer satisfaction scores |

---

**FIG. 5 Participant demographics & characteristics: India**

<table>
<thead>
<tr>
<th>Number of participants</th>
<th>Diary studies</th>
<th>Interview participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Gender</th>
<th>Females</th>
<th>Males</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>60%</td>
<td>55%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Age distribution</th>
<th>18-34</th>
<th>35-64</th>
</tr>
</thead>
<tbody>
<tr>
<td>95%</td>
<td>5%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Union membership</th>
<th>0%</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Education level</th>
<th>Secondary (Class XII)</th>
<th>Bachelor's degree</th>
<th>Post-graduate degree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
</tbody>
</table>

---
**SUB-SAHARAN AFRICA**

**ROLE**

**FULFILLMENT**

Software used in annotating videos to provide AI model training data; enables workers to annotate an object in one frame, and have the annotation of that object continue through many frames. Previously workers had to annotate the object in each frame of the video.

Software used in annotating images, allows workers to select the far corners of the object that needs to be annotated, and the tool will draw the rest of the contours around the object.

**COACHING**

Real-time performance feedback

Software used to review the accuracy of annotations. Approves or rejects, does not provide any kind of feedback or coaching on what needs to be improved.

---

**FIG. 6 Participant demographics & characteristics: Sub-Saharan Africa**

<table>
<thead>
<tr>
<th>Number of participants</th>
<th>41 Diary studies</th>
<th>28 Interview participants</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>59%</td>
<td>57%</td>
</tr>
<tr>
<td>Male</td>
<td>41%</td>
<td>43%</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under 35</td>
<td>97%</td>
<td>96%</td>
</tr>
<tr>
<td>35-64</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Union membership</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Members</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td><strong>Education level</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Some post-secondary</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Completed post-secondary</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>Some college/University</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>College/University</td>
<td>8</td>
<td>12</td>
</tr>
</tbody>
</table>

Legend:
- Diary study only
- Diary study & interview
### UNITED STATES

<table>
<thead>
<tr>
<th>ROLE FULFILLMENT</th>
<th>Real-time task assignment</th>
<th>Handheld scanner task assignment: Device and software used to complete tasks (e.g., give workers instructions to guide the movement of items throughout the warehouse, or which trucks to load packages onto)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROLE FULFILLMENT</td>
<td>Task augmentation</td>
<td>Return processing hardware and software: Device and software to assess condition of returns, and direct worker on next steps for item (e.g., repackage, dispose)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Robotic item movers: Robots deliver items to pickers, packers, and stowers, reducing or eliminating the need for humans to move around the warehouse to complete these jobs or carry heavy loads</td>
</tr>
<tr>
<td>COACHING</td>
<td>Real-time performance feedback</td>
<td>Handheld scanner feedback: Device and software used to complete tasks also provides information on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Whether tasks have been correctly completed (e.g., the worker has found the correct item, placed the item in the correct location, or loaded the package onto the correct truck)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The worker's speed of task completion (how long between completing one task and the next), and number of tasks completed per hour</td>
</tr>
<tr>
<td>PERFORMANCE EVALUATION</td>
<td>Performance target setting</td>
<td>Software that sets targets for worksite based on historical performance and company goals</td>
</tr>
<tr>
<td></td>
<td>Performance assessment</td>
<td>Software tracks performance against targets, warns worker and notifies management when performance lags for too long</td>
</tr>
</tbody>
</table>

**FIG. 7 Participant demographics & characteristics: United States**

<table>
<thead>
<tr>
<th>Number of participants</th>
<th>17 Diary studies</th>
<th>8 Interview participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>41%</td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>59%</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under 35</td>
<td>65%</td>
<td></td>
</tr>
<tr>
<td>35-64</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Union membership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Members</td>
<td>23%</td>
<td></td>
</tr>
<tr>
<td>High school/GED</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Current college student</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Trade/Vocational school</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>College</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Race**

<table>
<thead>
<tr>
<th>Race</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>White/Caucasian</td>
<td>4</td>
</tr>
<tr>
<td>Black/African-American</td>
<td>3</td>
</tr>
<tr>
<td>African</td>
<td>1</td>
</tr>
<tr>
<td>Asian-American</td>
<td>0</td>
</tr>
<tr>
<td>Biracial/Multiracial</td>
<td>3</td>
</tr>
</tbody>
</table>

US participants were asked to describe their race/ethnicity in a freeform entry. In order to more easily show the representativeness of the participants in the US site along this demographic dimension, we have combined participants into more general descriptions in this chart. White/Caucasian in the chart includes participants who answered “White,” “Caucasian,” and “White (Irish and German).” Black/African-American includes participants who answered either “African American” or “Black.” Biracial/Multiracial includes participants who answered “Biracial,” “African American and Caucasian,” “Mixed ethnic origin,” “Caucasian,” and “African American and Puerto Rican.” All other labels (Asian-American, African) are descriptions directly offered by participants.
APPENDIX 2

Research Methodology

Research methods

The themes and recommendations from this report are grounded in a literature review of related subjects, as well as primary research with workers at each site, virtually fielded from November 2021 until March 2022. All research was conducted in English, unless noted below. Where the literature revealed opportunities to better understand AI’s impact on job quality and worker well-being, we incorporated these areas into guides for diary studies to be completed by participating workers. These diary studies then served as a foundation for a series of semi-structured interviews with diary study participants at each site.

Participants shared their reflections on the diary study questions and prompts through a combination of text, voice, and video answers, as well as image responses to a limited number of questions. To better understand themes emerging from the diary studies, a subset of the diary study participants were each invited to participate in a 60-minute semi-structured interview via Zoom where they were asked a combination of universal questions about emerging themes as well as specific questions about their diary study and interview responses. All research was conducted in English except where noted below. The participants had high degrees of competency in English due to living in countries where English is frequently spoken, using it as the main language in their jobs, or both. For the participants based in India, these interviews were conducted one-on-one in English with the primary researcher. A translator fluent in Hindi was also on the call to offer translation support if requested by participants. US interviewees participated in one-on-one Zoom calls with the primary researcher.

Unlike the other sites, participants in the sub-Saharan Africa site were colleagues. To prevent the possible appearance of choosing favorites by selecting only a subset of participants for interviews, all participants at this site who completed the diary study were invited to participate in interviews. Due to strong interest from the participants who completed the diary study and comparatively limited research team time, these interviews were structured as group interviews with three to four participants per group. Due to last-minute schedule changes from participants, the actual number of interviewees per group ranged from one to four. The research team explored possible upsides and downsides of this approach with leads from the sub-Saharan African group, who offered guidance that this approach should work well; employees were used to participating in focus groups and other similar discussions with each other. This participant site included several individuals with team/project management, mentorship, or coaching responsibilities. Each of these individuals was interviewed one-on-one to ensure that they could speak freely about aspects of their managerial, supervision, or mentorship duties they might prefer not to discuss in front of potential reports. Similarly, this design ensured that workers could speak about experiences they might prefer not to share or discuss with managers or supervisors.
Participant recruitment

For this work, the research team sought to include a wide range of possible workers who frequently use or interact with AI in their workplaces with a focus on workers who were structurally likely to be more vulnerable to any harms from these technologies. We sought to learn from:

- Vulnerable workers in a high income country (e.g., workers with fewer formal education credentials and thus fewer opportunities for higher paying jobs)
- Middle class workers in a LMIC (e.g., workers who were less vulnerable in the context of their own country, but could be substantively affected by global market changes driven by decisions abroad or in high income countries)
- Working class or working poor workers in a LMIC (e.g., workers who could be both individually and collectively affected by the forces described for the prior two sites, and thus at highest risk of harm).

The team considered three possible approaches for recruitment:

<table>
<thead>
<tr>
<th>Recruitment Approach</th>
<th>Advantages</th>
<th>Disadvantages and Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working with an independent research recruiter</td>
<td>Workers could participate independently of their employer</td>
<td>Participants would need their anonymity protected to ensure their employers would not punish their participation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of employer permission might make participants feel less comfortable speaking frankly about their experiences.</td>
</tr>
<tr>
<td>Collaborating with a supportive employer</td>
<td>Workers participate with their employer’s full permission</td>
<td>Participants’ individual and collective ability to participate voluntarily and speak freely would need to be protected through confidentiality and anonymity provisions.</td>
</tr>
<tr>
<td>Collaborating with a worker organization or union</td>
<td>Workers could participate independently of their employer</td>
<td>Employers often scrutinize organizers and active union participants more heavily, increasing their possible risk of participation and the importance of protecting their anonymity.</td>
</tr>
<tr>
<td></td>
<td>Workers would likely have higher familiarity with how technologies affect working conditions and more</td>
<td>High levels of familiarity with technology’s impacts built through organizing work might not be representative of the broader group of workers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Worker organizations/unions are rare or non-existent in the LMIC occupations that work closely with AI technologies.</td>
</tr>
</tbody>
</table>
Due to the nature of the research, there was no ideal set of sites to conduct this work. Each approach would require: (a) setting up provisions to protect participants’ ability to voluntarily participate and speak freely, and (b) attention by the research team to ensure the representativeness of the participant pools and the perspectives they shared. The team ultimately decided against recruiting through worker organizations and unions, due to the difficulty of this approach in the LMIC site, and concerns about representativeness in the high-income country.

For the participants based in India and the United States, we worked with a professional research recruiter to identify and invite qualified participants for the study. Participants were recruited through advertisements and targeted outreach.

For the participants based in sub-Saharan Africa, we collaborated with a company which was developing a series of ML tools to assist their data annotators in completing their work. This company agreed to identify a group of employees who were experienced in using these tools and to forward them an introductory note from the research team which outlined the research and invited participation. Participation was entirely voluntary — not required or encouraged by the company, as was made clear in the introductory note. If participants were interested, they were asked to sign up and participate on their own time, using their personal phones or devices (rather than during their work hours, using company devices). The note was forwarded to the group’s personal email addresses (not their work addresses) to further underscore the independence of the research and voluntary nature of participation.

All participants at all sites were compensated for their time, with interview participants receiving an additional amount for their additional time. Compensation amounts were set to be generous relative to participants’ normal hourly wages, without being so high as to create undue pressure on participants to join the study (and thus potentially undermine the voluntariness of their participation).

**Ethics and informed consent**

In line with best practices in qualitative research, each participant in the study was informed of the goals, content and format of the study, the benefits and risks of their participation, and the organization and individuals responsible for the study. They were additionally informed that any stories or quotes shared in public research outputs would be anonymized to protect their identity and mitigate any risks of their participation. All participants digitally signed consent forms confirming that they received and understood the information about the study and that their participation was entirely voluntary and could be withdrawn by them for any reason at any time. They were also reminded of this at the outset of each interview, where they were also informed that they could choose to decline to answer any questions posed to them and choose to end the interview at any time.
Since the introduction to the participants at the sub-Saharan Africa site was performed by participants’ employer, additional information was included in the call for participants and the consent form for that site to clarify that the research was being conducted and managed by an external group. The call for participation also included the confidentiality protections participants could expect, namely that their individual responses would not be shared with their employer. The participating company additionally signed a memorandum of understanding in advance of embarking on the study confirming that: (a) no individual or attributable data from participants would be shared with them, and (b) any information shared with them from the research would be synthesized and shared in the form of high-level themes.

For each site, the research team at PAI was the only group with access to participants’ diary study and interview responses. In the case of group interviews, participants agreed at the start of interviews to keep any comments shared by others in the group confidential and to protect the privacy of other participants. In line with standard qualitative research practices, the employers at all sites are not named, to assist in protecting the anonymity of participants.

Confidentiality and data storage

All participants’ identities have been anonymized in the research output. After completion of the diary studies and interviews, participant responses have been stored separately from identifying information about the participants who provided them.

Data analysis

Information from this study has been analyzed using two approaches. To determine a framework of workplace AI product types from workers’ perspectives and to categorize the technologies mentioned in this study according to the framework, a deductive approach was used. To identify themes from the participant responses, an iterative inductive approach was used both to identify initial and emerging themes and to synthesize and cluster those initial themes into the major themes in this report.
References


Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0186
Comment on FR Doc # 2023 12995

Submitter Information

Email: [Redacted]
Organization: The Center for Law and Social Policy

General Comment

See attached file(s)

Attachments

FINAL CLASP OSTP RFI 062923
June 29, 2023

White House, Office of Science and Technology Policy
Executive Office of the President
Attn: Alan Mislove, Assistant Director for Data and Democracy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Request for Information on Automated Worker Surveillance and Management

Submitted at: https://www.regulations.gov/commenton/OSTP_FRDOC_0001-0008

Dear Mr. Mislove:

On behalf of the Center for Law and Social Policy (CLASP), I submit these comments in response to the White House Office of Science and Technology Policy’s (OSTP) Request for Information (RFI) on Automated Worker Surveillance and Management, dated May 2, 2023. CLASP thanks the White House and OSTP for seeking comments on this fundamental and insidious issue of workers’ rights.

Importance of Worker Surveillance and Management to The Center for Law and Social Policy

The Center for Law and Social Policy (CLASP) is a national, nonpartisan nonprofit advancing anti-poverty policy solutions that disrupt structural, systemic racism and remove barriers blocking people from economic justice and opportunity. With deep expertise in a wide range of programs and policy ideas, longstanding relationships with anti-poverty, child and family, higher education, workforce development, and economic justice stakeholders, including labor unions and worker centers, and over 50 years of history, CLASP works to amplify the voices of directly impacted workers and families and help officials design and implement effective programs.

CLASP seeks to improve the quality of jobs for low-income workers, especially workers of color, women, immigrants, and youth. Our work includes working with policymakers to raise wages, increase access to benefits, implement and enforce new and existing labor standards and ensure workers can strengthen their voice through collective bargaining. Quality jobs enable workers to balance their work, school, and family responsibilities—promoting economic stability and security.

Our comments on the importance of worker surveillance and management will address the compounding ways that algorithmic management lower job quality, specifically focusing on:

1. Pace-of-work and surveillance’s increasing effect on workers’ physical and mental health
2. Algorithmic management’s effects on scheduling and employee misclassification
3. Algorithmic management’s obstruction of the right to organize.
4. Algorithmic management’s role in occupational segregation and workplace discrimination through hiring and discipline

These comments will describe the threats that algorithmic management and surveillance pose to the future of work, as well as propose some policy solutions from the local, state, and international level that policymakers can use to prevent or mitigate those harms.

A. Background

Technological innovation has always been a central determining factor of job quality. Technological innovation alters the scale of production, and since workers are an essential part of production, any change in scale necessarily impacts workers. Technology can be used to reduce labor costs, increase production, and otherwise control workflows and the workforce. Often, researchers and policymakers discuss automation as a looming threat we must tackle before it overwhelms us. In reality, harnessing new technologies to increase production has always been a central strategy of colonialism, shaping the very creation of the United States. We cannot untether economic progress from the brutality of slavery. The invention of the cotton gin allowed slave owners to expand their land and use slave labor to grow more cotton. This innovation was developed on the backs of slaves who were pushed to pick more as crops expanded exponentially — in 1810, there were 87,000 cotton spindles, and by 1860, there were five million. What we consider “cutting-edge” technological revolutions and sleek management systems can oftentimes be traced back to techniques developed by plantation owners to increase profits.¹ Slave owners relied on technological innovation coupled with brutal punishment and constant surveillance in an attempt to extract every ounce of labor possible.² When historicized through racial capitalism, innovations like Henry Ford’s invention of the assembly line in 1913 come into view as potential tools of worker oppression. His invention, which allowed for work to be broken down into discrete tasks per employee, revolutionized manufacturing and took the time to assemble a Model T chassis from 12.5 hours to just 1 hour and 33 minutes.³ This scaling of production became widespread; soon most major companies were operating with some sort of assembly line, even if they weren’t manufacturing-based. And with it, the number of employees needed, the number of cars produced, and the pace of work were fundamentally changed.

This speeding up of production through automation cannot be considered in a vacuum. It is coupled with other fundamental changes in the structure of our labor—namely, the decline in unions and the rise in workplace fissuring and the platform economy. In the early 1900’s, union rates remained low—between 10 and 12 percent. In 1935 with the passage of the National Labor Relations Act, union membership rates began to skyrocket, from 10.8 percent in 1935 to 33.4 percent in 1945.⁴ With the rise of collective bargaining came an increase in higher quality jobs. But the passage of the Taft-Hartley Act in 1947 and its provision allowing states to pass right-to-work laws significantly stymied union power. In the decades since 1947’s high, union membership rates have continuously dropped, with current rates even lower than:

---

they were before the 1935 passage of the NLRA. However, low unionization rates are not indicative of workers’ rejection of unions. Most recently, union support has been high. In 2022, union approval rates hit a peak of 71 percent, a high not seen since 1965, yet only 10.3 percent of US workers are represented by unions. This is due to aggressive union-busting on the side of employers, of which surveillance is often a main method. In 2022, the rate of employers charged with unfair labor practices rose 16 percent over the 2021 rate, and with the National Labor Relations Board facing underfunding and understaffing, workers have little recourse to fight back against oppressive working conditions.

Simultaneously, the workplace has fissured. Alongside technological innovation, fissuring occurs when companies attempt to shed costs by outsourcing and contracting non-central aspects of its work. Focusing on saving costs and increasing revenue, companies look to remain lean and use third-party contractors to drive costs down. This can look like outsourcing customer service, janitorial services, human resources, and communications. But, as David Weil explains, fissuring doesn’t just involve partnering with a secondary employer. Rather, fissuring utilizes subcontracting, franchising, third-party management, and employee misclassification to shed the main responsibilities of employment while remaining in control of profit, competition, and brand standards. By fissuring aspects of their company, lead companies are no longer responsible for maintaining labor standards, safety, offering benefits, or dealing with on-the-job issues. When competing for contracts for the outsourced business functions, contractors and subcontractors create a “race to the bottom” to win bids for the work, often on the backs of workers who see their wages and benefits slashed. The culmination of this new business model has solidified the gig economy as the expedient way to shed employment responsibility and increase profits.

Not having clear access to collective bargaining or having a good sense of who one’s employer is makes the employment relationship opaque; algorithmic management furthers this opacity by removing “humans from the loop” of decision-making, while simultaneously utilizing technological surveillance to create a constant feeling of monitoring (by what is now a shadowy boss). Algorithmic management affects all sectors, but low-wage and hourly workers across sectors—like the service industry, retail, warehouse and logistics, agriculture, hospitality, domestic work, healthcare, and the gig economy—are particularly primed for algorithmic management, as these jobs often involve more measurable tasks. Due to occupational segregation and systemic discrimination in our economy, marginalized workers such as workers of color, women, LGBTQIA+, and immigrant workers disproportionately hold these low wage, low quality jobs prone to higher levels of surveillance. Algorithmic management in occupationally segregated industries can be traced back quite clearly to slavery; a lack of social power combined with constant surveillance; the extraction of one’s bodily data and autonomy for the sake of profit, are all standard practices in algorithmic management that make data “the new cotton.”

B. Defining Algorithmic Management and Surveillance

---

5 Ibid.
What makes algorithmic management unique—and what makes this moment one in which the United States must take particular action—is not the usage of technology in itself, but the way in which technology is increasingly used to make decisions. Algorithmic systems are now being used explicitly to make workforce and workplace decisions, oftentimes without human assistance.

In her October 2022 memorandum, National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo defined algorithmic management as “a diverse set of technological tools and techniques to remotely manage workforces, relying on data collection and surveillance of workers to enable automated or semi-automated decision-making.” We use this definition in our assessment of algorithmic management, as it leaves room for the myriad ways management and surveillance show up in the workplace.

The age of closed-circuit television (CCTV) and using cameras to monitor workers on the job has long passed. Now, enormous amounts of data are collected from as many different sources as possible; this data is then processed into an algorithm that aggregates it, and then rates human performance and makes decision based on the data received. Because algorithms rely on as much data as possible, this has led to a proliferation of surveillance tools.

Workplace surveillance can be physical, mental, and digital. Physical surveillance intends to track both the physical location of workers, such as using GPS-based applications to track delivery vans or trains. Wearables can allow warehouse workers to be tracked as they move through a worksite. Amazon became notorious for its use of “time off task” (TOT) tracking to enforce draconian break policies within its warehouses. Sociometric badges can track workers’ proximity to other employees, tracking who interacts with whom. Additionally, not only the location of one’s body in a workplace, but the pace of work and its effect on the body can be tracked through biometric feedback, as well as using point-of-sale (POS) and QR-codes to tie employee identification to their product and how quickly it moves along.

In their effort to create as many data points as possible, employers have attempted to monitor employees’ mental status as well. This can take the form of using sociometric badges to track heart rate and its relation to stress, or tracking vocal speech patterns in an attempt to identify when workers are frustrated or calm in a service environment. While seemingly the stuff of science fiction, a booming industry of “neuro-surveillance” looks to use microprocessors to decode productivity via electrical signals in the brain.

Mental surveillance is very closely related to the third form of surveillance, digital surveillance. This involves tracking what employees do on the Internet in an attempt to not only monitor but predict their

---

14 Constant Boss, 13.
behavior. This practice had been used for decades for platform workers but became widely known as office workers became remote during the COVID-19 pandemic and found themselves being subjected to keystroke, camera, application, and browser history monitoring, and more to ensure that workers were staying on task.¹⁶ Digital surveillance is also used to make hiring decisions. Data from personal social media accounts is regularly used to evaluate candidates; more recently, facial recognition and emotional monitoring is being used in interviews to judge candidates’ performance. Within the workplace, web history is being used in an attempt to predict when workers will take time off, organize, or consider finding new work.¹⁷

1. Methods of Algorithmic Management & Their Consequences

A. Surveillance & Pace of Work

Algorithmic management is a continuation of past technological innovations that were aimed at increasing productivity. Historicizing recent technological developments in this way allows us to identify production standards as a driving force proliferating new surveillance methods. It is not simply that employers are monitoring their workers. In fact, an end to camera surveillance, wearables, and certain other physical tracking would not mean an end to surveillance altogether. This is because surveillance of the worker often occurs through acute surveillance of a product and the means of production. Across industries, QR codes, barcodes, point of sale (POS) and other product-tracking methods are being used in addition to surveillance of individual workers like the methods listed above. Workers are effectively tied to their products to promote productivity at the cost of worker well-being.

The ubiquitous business practice of surveilling production is based on the lean production model. Emerging out of auto manufacturing through Toyota in 1948, lean production is a system based on the philosophy of “achieving the complete elimination of all waste in the pursuit of the most efficient methods.”¹⁸ One of the biggest methods within the Toyota Production System is “just-in-time” manufacturing, which requires precise tracking of parts and inventory, as well as careful coordination of resources, including employees. It requires that only the minimum amount of anything should be on hand, essentially stripping the workforce down to its barest needs in what has since been described as “management-by-stress.”¹⁹ This model began in the auto industry but is now present in every conceivable industry and sector, rebranded as “six sigma” and making up a profitable business coaching industry. Now, only 23 percent of reported users of this form of management are within manufacturing; the majority (77 percent) come from the service industry.²⁰

While lean production has been the modus operandi of business for decades, algorithmic management has allowed lean production to grow exponentially, unchecked by human management. Algorithmic

---

management allows both the worker and their product to be consistently monitored, second-by-second. In fact, employers consistently use algorithmic data to inform just how many seconds a certain task should take. In talking to Starbucks workers located in Memphis, Tennessee, we discovered that drive-thru employees were expected to complete window interaction in 45 seconds or less. This was tracked through their login to the point-of-service (POS) register and was standardized through algorithmic monitoring of the fastest time recorded through aggregated POS data. Even if it took only an additional second, workers who did not hit this standard were disciplined.21 One worker said, “You’re not given the tools, but you gotta get these numbers, and then at the end of the month, they’re like ‘well, why didn’t you hit the numbers?’ How? It’s impossible!”22

Algorithmic management is present in warehouse and logistics as well. Both Amazon delivery drivers and Amazon warehouse workers have described the widespread use of productivity measures relying on algorithmic surveillance through wearables and GPS, which penalize them for time-off-task (TOT). If an employee’s TOT exceeds 15 minutes, or one’s rate of productivity falls below the prescribed speed for the task (often seconds), an Amazon worker will get an automatic write-up. Visits to the restroom, human interaction with other employees, or any sort of rest tracked through the wearables is counted as TOT. Ilya Geller, who worked at Amazon as a stower, said, “you’re being tracked by a computer the entire time. You don’t get reported or written up by managers. You get written up by an algorithm.”23

Pace of work surveillance threatens workers’ physical health and safety. Workplaces with higher levels of surveillance and lean production face higher rates of workplace injury. Amazon warehouse workers, for example, were found to suffer serious injuries at twice the rate of rival companies in 2021.24 Amazon’s “relentless push for e-commerce dominance” led to increased injuries both inside and outside the warehouses.25 Amazon delivery drivers, faced with GPS-tracking that significantly squeezed them to deliver packages faster, got into more than 60 accidents between 2015 and 2019, leading to 10 deaths.26 Pushing workers beyond reasonable limits to deliver as fast as possible often comes with deadly consequences. However, as many of these drivers were independent contractors—another cost-saving measure on Amazon’s part—Amazon was not found responsible for the accidents.

Algorithmic management’s pace of work also leads to intense mental duress. With an inhumane pace of work, as well as chronic understaffing to drive down costs and speed up production, workers find themselves overworked and isolated in traditionally underpaid industries. This effect has commonly been coined as job strain, which has been shown as strongly linked to depression, anxiety, and higher rates of suicidality. In 2019, suicide rates at the workplace rose to 307, a 39 percent increase since 2000.27 In our interview with Starbucks workers, one barista expressed to us the emotional toll this job strain took on

21 Kylie Throckmorton, Starbucks Worker, Interview 2022.
22 Nikki Taylor, Starbucks Worker, Interview 2022.
26 Ibid.
them: “I would come home, and throw stuff and cry, and scream . . . that was my struggle—between knowing that I deserved better and not being able to leave everyone else in the pits of hell.”

**Interventions**

Using algorithmic management to dictate an inhumane pace of work leads to eroding job quality while simultaneously producing higher profits for corporations. Despite, or perhaps because of its presence as a commonplace business tactic, algorithmic management and lean production are relatively unstudied as a topic for policy intervention. However, there are many useful avenues that the federal government can take to begin to combat the effects of pace of work issues enabled through surveillance:

**Regulatory Recommendations:**

- **Issuing OSHA Guidance:** Governing for Impact recently proposed action memos to OSHA outlining their statutory authority to address workers’ mental and physical health as they relate to ergonomic standards. We urge OSHA to issue rules regulating the use of surveillance in the workplace due to its risk of job strain on workers’ mental and physical health. In doing so, these regulations should comprehensively identify workplace injuries due to job strain and algorithmic surveillance practices on a sector-by-sector level, strategically focusing on industries that have a high rate of OSHA violations paired with a low rate of incident reporting.

- **Funding NIOSH Research:** We support the funding of NIOSH to pursue research related to job strain as it relates to electronic surveillance. This will allow legislators to act based on scientific research to complement worker narratives. Specifically, we consider the following questions as central:
  - How does job strain present itself across sectors and within specific types of work?
  - Across sectors, does job strain have a negative correlation with increases in wages and benefits?
  - What long-term physical and mental conditions arise in workers affected by surveillance and algorithmic management-based job strain?
  - Under what conditions does increased pace-of-work lead to more frequent workplace accidents?
  - Does the risk of workplace accidents suggest a clear limit on the “safe” pace of work for workers in particular industries or workplaces? What might the threshold be?
  - What criteria can be created to establish guidelines for when job strain due to surveillance, algorithmic management, and pace-of-work increases reaches said threshold?

- **Using an Inter-Agency Approach:** We support General Counsel Abruzzo’s 2022 memo on unlawful electronic surveillance and automated management practices and agree that an inter-agency approach that includes the Federal Trade Commission and Department of Justice in creating new standards is paramount.

---

28 Nikki Taylor, Starbucks Worker, Interview 2022.
Policy Recommendations:

- **Hold Corporations Accountable:** New corporate accountability legislation could require greater transparency over lean production and surveillance methods, as well as requirements that data-driven technology be continuously evaluated by outside legal entities, including impact assessments. Additionally, workers should have a role in impact assessments, as experts of their workplace who can speak to how algorithmic systems are affecting their work life.\(^{31}\)

- **Protect Data Privacy:** Data privacy rights, like the Worker Privacy Act proposed by the Center on Privacy & Technology at Georgetown University Law Center, can limit the amount and types of data employers can collect.\(^{32}\) Currently, there are very few limits on data collection, and little to no privacy rights for workers. Experts suggest that a comprehensive federal data privacy law, similar to actions taken in California, could begin to bring transparency back to the workplace.\(^{33}\) Additionally, workers having knowledge of what data is being collected and how it informs things like quotas, productivity scores, and “time-off-task” rates can give them power to speak out against inhumane or retaliatory treatment.

B: Algorithmic Scheduling and Employee Misclassification

Combined with lean production methods, scheduling via algorithm creates a rigid workplace that offers little flexibility to workers. “Just-in-time” scheduling is increasingly automated thanks to a booming industry of automated human resource companies and scheduling apps like Kronos, WhenIWork, Legion, Clockify, and more, which promise to eliminate human decision-making bias and promote efficiency in scheduling. These apps—which make up what is estimated to be a $530 million dollar industry—automate scheduling by using forecasting models that are integrated with point-of-sale software.\(^{34}\) For example, a retailer can use software like 7shifts, which will aggregate data from previous months, years, seasons, and even by tracking where Square customers have swiped their cards nearby, to create a type of “staffing forecast.” The algorithm will then recommend the minimum number of employees needed to operate that shift based on that data-driven forecast.\(^{35}\) This method of scheduling, coined “refractive surveillance,” far exceeds the methods and capacity of manual scheduling and has brought “on-call” scheduling to virtually all industries.\(^{36}\)

Scheduling practices are already a main concern of job quality policy. In 2020, new survey data revealed that over half of surveyed workers regularly “clopened,” meaning they consecutively closed and opened

---


\(^{33}\) Constant Boss, 27, and The California Consumer Privacy Act, as originally introduced, provided data privacy rights for employees, independent contractors, and job applicants but these categories will be exempted from the final legislation until 2022; see https://oag.ca.gov/privacy/ccpa.


the following day.\textsuperscript{37} Doing so leaves little rest time between shifts, and beyond exhausting workers, can make it difficult to find childcare, schedule shifts at other jobs, and otherwise plan one’s life. Workers in low-wage industries already have very little control over their schedules. A survey of Los Angeles retail workers found that 44 percent of workers experienced schedules fluctuating more than 10 hours between weeks.\textsuperscript{38}

By following “just-in-time” principles, workers are left with little time to plan their lives, including rest, childcare, commute, and oftentimes scheduling shifts for secondary jobs.\textsuperscript{39} This is especially difficult for part-time workers, many of whom are marginalized workers in low-wage sectors where full-time work is difficult to find. Part-time workers are more likely than full-time workers to have erratic hours, resulting in volatile incomes. Automating scheduling, while cutting costs and improving efficiency, allows an algorithm to change schedules on short notice, widely changing how many hours a worker can get per week, all in response to consumer forecasting data that is often hidden from workers.

The aforementioned applications use what the railroad industry refers to as “precision-scheduling” to attempt to predict how lean a workplace can get while managing forecasted demand. This, coupled with the increased pace-of-work, increasingly leads to tragedies like those mentioned previously. In the railroad industry, for example, algorithmic models have seen trains become longer, sometimes up to 3 miles long, while railroad staff has drastically decreased to skeleton crews that work multiple-day shifts. Workers are essentially on call for days, and operate with little to no rest, waiting for trains to have enough cargo as determined by an algorithm to be deemed profitable.\textsuperscript{40} This has led to disastrous derailments—in 2019, there were 341 derailments on main lines, and of those, 24 were freight trains carrying over 159 cars of hazardous materials.\textsuperscript{41} This method of “Precision-Scheduled Railroading” (PRS) is used by almost all Class I railroad companies, up to 94 percent of the freight rail industry’s revenue.\textsuperscript{42}

Scheduling does not only mean shift-to-shift assignments. Rather, algorithmic scheduling allows employers to track not only a workday, but an individual employee’s work life second-by-second. Algorithmic systems allow for employers to track time off task and dock employee pay, so that workers often only get paid while they are actively working.\textsuperscript{43} Additionally, algorithmic scheduling often uses performance metrics and incentives for scheduling—such as with assigning rides or deliveries for Uber or Doordash—that are unclear to workers.\textsuperscript{44} This means that workers’ pay is often as unpredictable as their schedules themselves. Algorithmic scheduling makes compensable time unclear to workers and allows employers to maximize time spent working while minimizing pay.

\textsuperscript{38} LAANE & UCLA Labor Center, \textit{Hour Crisis: Unstable Schedules in the Los Angeles Retail Sector}, 2018.
\textsuperscript{42} Ibid.
The opacity of scheduling software is oftentimes compounded by an opacity in the employment relationship itself. With the rise of workplace fissuring and the gig economy, workers are often unaware not only of what information is being used to make decisions in their workplace, but who is making the decisions in the first place. Employers utilizing fissured structures oftentimes use technology to further distance themselves from their employees. Just like other fissuring methods—such as subcontracting, franchising, and third-party management—algorithmic management allows employers to maintain control over standards and productivity while creating an illusion of worker independence. This is often achieved through combining surveillance and automation with illegal misclassification. By misclassifying workers as independent contractors, federal labor protections no longer apply to these workers. Companies then create more murky layers of automation—like automated HR, algorithmic scheduling, and automated management decisions—to cement the illusion that the worker is in fact working independently, and that decisions are being made based solely on the individual worker’s performance metrics. In reality, the lead company is in control of how the work gets done, when it gets done, and all aspects of job quality—all while absolving themselves from responsibility for any of it.46

The narrative of “worker flexibility” that often comes from algorithmic management software is another layer of removal from corporate accountability. And, with the lack of federal oversight, combining fissuring and surveillance is being applied beyond its platform origins—healthcare workers, childcare workers, retail, grocery, and fabrication workers have all seen attempts to misclassify workers while controlling them through surveillance.47

**Interventions:**

**Regulatory Recommendations:**

- **Staffing Ratios:** Using algorithmic consumer forecasting can be tempered through stronger regulations on staffing ratios. Staffing ratios have long been the concern of nurses and teachers unions. Recently, the Centers for Medicare & Medicaid Services (CMS) launched a Request for Information and proposed rulemaking for guidance on safe staffing ratios for nursing homes.48

  Incorporating algorithmic scheduling within our understanding of how staffing ratios get determined could help mitigate these issues. Additionally, safe staffing regulations should not only consider the length of hours and number of employees, but the way in which scheduling produces job strain as described above. For example: facing decreased staff, yet increased workloads, hotel workers organized to pass an ordinance in the City of Los Angeles not only requiring panic buttons for safety, but dictating the amount of square footage a hotel worker is expected to clean

---

45 *The Fissured Workplace.*


per shift. Similarly, California’s AB 701 prohibits excessive work pace in warehouses and distribution centers and requires transparency for quotas used to determine pace.

- **Employer Status Guidance:** The Department of Labor’s proposed rule on independent contractor classification under the Fair Labor Standards Act (FLSA) from October 2022 should clarify within the rule’s economic reality test that algorithmic management and supervision is evidence of employer control and employee status.

- **Compensable Time Guidance:** DOL’s Wage and Hour Division can release guidance on how compensable time is determined for algorithmically managed workers. By updating guidance to reflect the way that algorithms separate out different tasks, DOL can not only help ensure that workers are being paid for all time spent working but can ensure that workers who are under algorithmic management have more transparency around how their pay is actually calculated.

**Policy Recommendations:**

- **Include Algorithmic Scheduling in Fair Scheduling Laws:** Fair scheduling laws have been passed in multiple localities such as Chicago, IL; New York City, NY; Seattle, WA; San Francisco, CA; Philadelphia, PA; and Emeryville, CA, to name a few. These laws have seen markedly beneficial results: a two-year study of Seattle’s Secure Scheduling Ordinance found that workers’ knowledge of their schedule at least 2 weeks in advance increased by 11 percent; there was also an 11 percent increase in reports of good sleep quality and a 10 percent decrease in the likelihood of experience material hardship. Supplementing these gains by including algorithmic scheduling in these laws will lead to more positive benefits for workers. On the federal level, the Schedules That Work Act and Part-Time Workers Bill of Rights can consider algorithmic scheduling as a major part of their bills.

- **Protect Workers’ Rights to Organize:** Ultimately, issues of scheduling have most traditionally been dealt with at the industry level through collective bargaining. As we will detail in the next section, supporting legislation like the Protecting the Right to Organize (PRO) Act and funding the NLRB to strengthen worker’s ability to organize is one of the main ways to help address algorithmic management and shift the balance of power.

**C. Algorithmic Management and the Right to Organize**

Workplace surveillance fundamentally interferes with workers' right to organize in two major ways. First, surveillance is overtly used to identify organizers and workplace leaders, surveil union-planning, and use information to union-bust any attempt at an organizing effort. Secondly, the algorithmic methods listed above create unsustainable workplace conditions that lead to low morale, high-turnover, and isolation by pitting workers against each other. These conditions prevent workers from being able to come together to collectively organize.

---


Without having to hire union-busting detectives, new technology allows constant surveillance of workplace organizing, whether or not workers are actively seeking to unionize. Location tracking through wearables, keycards, and other biometrics have become sophisticated enough that employers can surveil interactions between coworkers, including with whom, where, how long, and sometimes even what was said.\(^5\) Additionally, employers can use “sentiment analysis,” personality assessments, and the tracking of personal social media profiles outside of the workplace in order to identify workers who may be sympathetic to unionization, and then target surveillance or retaliatory actions toward these workers.\(^5\) Whole Foods has already used this sort of surveillance to create a “heat map” of over two dozen metrics that may predict which stores might unionize.\(^5\) Secondly, once workers who are sympathetic to unionization are identified, algorithmic management through rigid production quotas, “time-off-task” penalization, and overwork can either put strain on these workers to get them to quit, or punish them into silence.

As Aiha Nguyen describes in an interview with an Amazon worker, Rina, algorithmic surveillance is a practice that affects not only individual workers, but all workers in a workplace collectively, because data on a single individual is meaningless. It is when data is aggregated across workers to set a standard for activity that it becomes meaningful. In Rina’s case at Amazon, “time-off-task” (TOT) was a metric used not to judge a single individual, but the standard by which all workers were judged:

> “Rina mentioned that [TOT] is an important metric in her job. This metric can determine whether a worker keeps her job or not. At the same time, workers are not given clear direction on how to respond to TOT. According to Rina, one co-worker was fired because he didn’t take it upon himself to find more work when operations were slow. Thus, TOT serves not as a productivity measure, but as a means of creating insecurity so workers hustle or face the threat of termination.”\(^5\)

Targeted surveillance against union sympathies, or in retaliation to information received about unionization efforts, becomes compounded with just-in-time lean production methods and algorithmic management and scheduling to create workplaces where workers are overworked, stretched thin, and often fighting for hours, for quotas, and for their sanity on the job. This creates not only personal job strain, but a collective sort of job strain that can ensure low morale and high turnover—a union-busting situation in and of itself.

**Interventions:**

**Regulatory Recommendations:**

- **Surveillance as an Unfair Labor Practice (ULP):** The NLRB already has the power to protect workers who wish to engage in concerted activity, such as discussing their employment situation and raising work-related complaints under the National Labor Relations Act. General Counsel

---

\(^5\) The Constant Boss, 28
\(^5\) The Constant Boss, 27-8.
Abruzzo’s memo on electronic surveillance already warned of the chilling effect that surveillance can have on organizing efforts. By classifying these practices as unfair labor practices, and/or requiring employers to prove that they are necessary to accomplish a legitimate business purpose, the NLRB could confront these effects within the statutory power they already possess.

- Requiring Data Transparency in Labor-Management Relations: In Spain, new legislation requires platform companies such as Uber to provide labor unions with access to the algorithms used to manage their workforce. Allowing unions access to the same data that employers have will help level the playing field for building collective bargaining agreements that include limitations on algorithmic management.\(^\text{57}\) Doing so is critical to remaining in line with federal law which requires employers to bargain with workers and their representatives over “terms and conditions of employment.” Unions need the ability to fully understand the “nature, scope, and effects of data-driven technologies” in order to properly bargain over them.\(^\text{58}\)

**Policy Recommendations:**

- Protecting the Right to Organize: Ultimately, outside of large-scale policy changes, the ability to collectively organize to negotiate better working conditions is one of the best ways for workers to challenge electronic surveillance and algorithmic management.\(^\text{59}\) Passing legislation like the Protecting the Right to Organize (PRO) Act can ensure that all workers can respond to the ways in which technology is affecting their working lives.

- Promoting Sectoral Bargaining: Internationally, trade unionism has been at the forefront of mitigating the harms of algorithmic management and electronic surveillance. Trade unions in the United Kingdom, for example, have negotiated with the government to form sub-committees to research algorithmic management; in Italy, trade unions negotiated on behalf of food-delivery platform workers to address algorithmic management.\(^\text{60}\)

- Investing in the NLRB: NLRB guidance on the use of electronic surveillance and algorithmic management will only be useful if the Board is proactively funded to be able to handle investigations into these practices. The federal government should proactively invest in funding capacity for not only responsive investigations, but to build out systems by which employers can be held accountable for demonstrating legitimate business purposes for their practices.

### D. Algorithmic Discrimination:

Algorithmic management also allows for employers to outsource hiring, discipline, and promotions. When it was first introduced, technological methods promised to remove human bias from decision-making through “fully automated decision-making.”\(^\text{61}\) But as algorithms are trained based on human decisions and human history, they are bound to replicate the discriminatory systems that already shape our

---


\(^{59}\) De Stefano 2020, 442.

\(^{60}\) Foresight Brief.

labor market. In hiring, algorithms are now being used to make decisions and screen hiring pools and resumes; on the job, algorithmic management and the increasing use of ratings and review systems can further impact who gets promoted or disciplined. Furthermore, an algorithm does not operate within a vacuum. Workers of color, women, immigrant, and LGBTQIA+ workers are already surveilled and discriminated against; algorithmic decision-making replicates structural biases and leads workers to continue to only be hired for jobs in low-wage industries where they will be further surveilled, perpetuating occupational segregation. As the algorithmic management industry booms, more and more companies are promoting tech with “predictive abilities,” claiming to be able to predict trustworthiness, responsibility, and other soft skills.

Algorithmic management’s lean production ethos can create job strain that is particularly difficult for workers with disabilities to keep pace with. Pregnant workers or workers with disabilities often need to adapt working conditions for their health, including taking more frequent breaks. One-fifth of pregnant workers reported having experienced pregnancy discrimination in the workplace. This potential discrimination is also not confined to the shop floor—digital surveillance allows employers to attempt to predict when workers are planning on taking leave for pregnancy; biometric surveillance can even allow employers access to fertility information. Speeding up pace-of-work through algorithms comes from aggregate information about the speed of an entire workplace. This means that workers with disabilities are being given productivity goals to fit the physicality of the aggregate, non-disabled workplace. Increasing the pace of work and eliminating breaks is also well-documented as negatively affecting mental health, further exacerbating stress felt by workers who may be neurodivergent, have anxiety disorders, depression, and other cognitive conditions. And because increased pace-of-work is often tied to automated discipline, promotions, and gamified rewards, workers with disabilities can end up being punished disproportionately. Furthermore, these management decisions are often being made by an algorithm that is using criteria unknown to the workers themselves.

Increasingly, an algorithm’s management decisions are being supplemented with customer reviews. Customer evaluations have long been a trend within delivery systems but are increasingly being used in other customer-facing industries and are now being used to make job quality decisions. For example, Amazon Flex delivery workers with higher ratings get preferred scheduling based not only on their delivery time, but also customer reviews. A report by Data & Society highlighted how drivers of color felt surveilled on the job not only by their employer, but by the community that they were delivering packages to. Often, this occurred through further technology systems, like the prevalence of Ring doorbell cameras in white communities. By allowing for community ratings to determine employee performance, employers replicate societal norms and can further racial discrimination. Additionally, because potential

---

62 Algorithmic Management Explainer, 14.
67 Algorithmic Management Explainer, 14.
bias in these cases originates not from the company, but from the customer, employers cannot as easily be held responsible for the bias that occurs, which happens often — facial recognition systems in the workplace are well-documented to have high error rates and racial biases. Ultimately, algorithmic management cannot escape the societal structures that create it.

Interventions:

Regulatory Recommendations:

- **Title VII Guidance:** The EEOC’s recent Title VII guidance on algorithmic practices in selection procedures is a critical first step for beginning to determine how technological surveillance and decision-making can have a disparate impact. Federal agencies should supplement existing guidance by outlining how algorithmic technologies can be used in ways that result in “disparate treatment” and intentional discrimination. Agencies should also outline ways that employers can take affirmative steps to apply a sociotechnical evaluation of their systems to assess for disparate treatment and/or disparate impact across the algorithmic lifecycle.

- **Title VII Enforcement:** Agencies should also prioritize enforcement actions against employers that engage in algorithmic discrimination. The EEOC and the Department of Justice should use innovative enforcement techniques such as algorithmic disgorgement to ensure that discriminatory models, and the data that they rely upon, are not accessible for further commercial use. Similarly, federal agencies must develop enforcement strategies that promote algorithmic transparency and affirmative notice to jobseekers that mitigate the impact of “black box” algorithmic opacity. Agencies must also consider rulemaking and other regulatory approaches that create heightened protections for the use of biometric data in algorithmic hiring platforms and related management systems.

- **Restricting or Banning Sentiment Monitoring and Pre-Hire Tests:** The EEOC requires employers to demonstrate the validity of pre-hire tests to defend against discrimination claims. The NLRB could similarly require that employers demonstrate legitimate business reasons for using monitoring, sentiment analysis, and tracking of workers’ social media. Technologies that fail to meet scientific validation or compliance with Title VII obligations should be treated as presumptively unlawful.

- **Regulating Customer Evaluations:** Title VII’s recent guidance clarifies that employers should often be responsible for algorithmic decision-making tools even when designed or administered by a third-party, like a software vendor. Similarly, the EEOC should consider the effects of customer reviews and evaluations as an employer responsibility. The means by which employers evaluate their employees should be their responsibility, no matter where the data is sourced from.

- **Clarifying Employer Compliance:** Currently, the ADA prohibits “standards, criteria, or methods of administration . . . that have the effect of discrimination on the basis of disability.” Pace of work standards should be considered a part of these “methods of administration” and should fall under


72 *Data and Algorithms.*

73 *EEOC Select Issues,* Question 3.

74 42 U.S.C. § 12112(b)(3)(A)
the ADA’s protection of disabled workers not being penalized for taking breaks or needing accommodations.

**Legislative Recommendations:**

- **The Black Worker Bill of Rights** outlines a set of rights necessary to combat racism in the workplace. One of the fundamental 10 rights is the “Right to Privacy and Freedom from Surveillance, Monitoring, Automated Management, and Control.”

- **Targeting Information Privacy:** Algorithmic management systems make decisions based on criteria unknown to the workers effected. Stronger data privacy laws could require that employers demonstrate reasonable business purposes for certain monitoring and demonstrate a lack of harm in data collection, similar to the Massachusetts Information Privacy Act. Legislation could also require data transparency so that workers are aware of what data is being used to make decisions, such as California’s 2018 consumer privacy legislation. These protections must apply with equal force to public-sector employers as they do private entities covered under federal antidiscrimination law.

- **The American Data Privacy Protection Act:** is a bipartisan legislative proposal that would create a comprehensive national data privacy legal framework for the United States. Key to the ADDPA are civil rights protections that prevent covered entities from collecting, processing or transferring data in ways that either discriminates against, or otherwise limits economic opportunities, for protected classes in select domains in addition to requiring algorithmic impact assessments. Similar strong legislative approaches to algorithmic discrimination include the District of Columbia’s Stop Discrimination by Algorithms Act.

**Conclusion**

The Center for Law and Social Policy encourages OSTP and the Biden-Harris Administration broadly to adapt current regulations and invest in new solutions to our rapidly changing work lives. Algorithmic management and surveillance are no longer novel forms of management or workplace experiments—they are rapidly becoming the standard way of structuring businesses and shaping workers’ lives. The federal government has a responsibility to summon its existing statutory power to create standards and practices around algorithmic management and surveillance, particularly for marginalized workers.

Respectfully submitted,

Nat Baldino, Policy Analyst

The Center for Law and Social Policy

---

Docket: OSTP TECH 2023 0004
Request for Information: Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0187
Comment on FR Doc # 2023 12995

Submitter Information

Email: [Redacted]
Organization: [Redacted]

General Comment

See attached file(s)

Attachments

Automated Worker Surveillance RFI.docx
June 28, 2023

Stacy Murphy
Deputy Chief Operations Officer/Security Officer
Office of Science and Technology Policy
Office of the President
The White House
725 17th Street, NW
Washington, DC 20503

Re: OSTP Request for Information: Automated Worker Surveillance and Management (OSTP Docket No. OSTP_FRDOC_0001-0004)

Dear Deputy Chief Operations Officer/Security Officer Murphy,

The National Partnership for Women & Families (National Partnership) is a nonprofit, nonpartisan advocacy group dedicated to improving the lives of women and families by achieving equality and equity for all women. The National Partnership promotes fairness in the workplace, access to quality health care and policies that help all people meet the dual demands of work and family. We ground ourselves in the lived experience of women and families, particularly those who face the greatest barriers to equity and opportunity. We accomplish our work through advocacy in both the public and private sectors and at the federal, state, and local levels. Our strategies include policy research and analysis; technical assistance to policymakers, media, and allies; leadership and participation in diverse coalitions and stakeholder relationships; public education, and public engagement. In all of our work, we seek to amplify the leadership of grassroots groups and women of color who are fighting for social justice.

The National Partnership’s work uniquely positions us to comment on automated worker surveillance and the ways that it impacts women, caregivers, disabled women, women of color, and women living at the intersection of multiple marginalized characteristics; data and evidence supporting the discriminatory use of this technology; information about the effectiveness of this technology; and potential policy and agency solutions.

Overview

The National Partnership applauds the Office of Science and Technology Policy (OSTP) for reaching out to the community for this feedback. As OSTP notes in its Request for Information, the use of automated manual systems is growing. Examples of automated worker surveillance include uses of webcams, screen monitoring, performance monitoring, tracking breaks, and monitoring for “productivity.”1 At the same time, these technologies can — and do — infringe

on the rights, needs, and safety of workers, particularly women workers, disabled workers,
workers of color, and other marginalized workers.

Part one discusses the ineffective nature of automated worker surveillance in achieving its
intended goals. Part two identifies the ways that automated worker surveillance leads to wage
theft. Part three identifies the ways that automated worker surveillance results in multiple forms
of discrimination. Part four identifies policy solutions on the legislative and regulatory fronts to
address the threats posed by automated worker surveillance.

Part One: Automated Worker Surveillance is Ineffective

Employers institute automated worker surveillance to track and ensure worker “productivity”
and to track worker performance. However, these technologies are not only overly invasive and
discriminatory — they also are not effective at achieving their intended purpose.

Many careers, such as care work, are not easily quantified.2 Yet, employers still attempt to collect
data to assess productivity and performance. For more service-based employers using emotional
recognition software, employees may actually change their habits to meet the demands of the
software as opposed to servicing the client.3 These changes may confuse customers and lead to
poorer customer service, as opposed to improving customer service.4

Workers also do not always understand the full extent of the surveillance.5 They may also not be
aware of exactly what contributes to data about their productivity or performance — scores may
be provided with no breakdowns.6 When workers do not understand what is being surveilled or
how it contributes to the determinations about their productivity or performance, it is difficult, if
not impossible, for them to make improvements. Instead, disciplinary action is taken with little to
no understanding of the concern at hand or how it could be rectified. Automated surveillance
may also cause anxiety, depression, and other mental health challenges for workers;7 decrease
morale8 and actually work to stifle productivity.9

---

from https://datasociety.net/wp-content/uploads/2021/05/The_Constant_Boss.pdf
3 Zickuher, K. (2021, August 18). Workplace surveillance is becoming the new normal for U.S. workers. Retrieved 1
June 2023, from the Washington Center for Equitable Growth website:
https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/
4 Ibid.
5 See note 2, p. 12.
6 Ibid., p. 18.
June 2023, from the BBC website:
https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers;
June 2023, from the Othering & Belonging Institute website:
https://belonging.berkeley.edu/blog-workplace-surveillance-harms-essential-workers
8 Ibid.
9 Ziegler, B. (2022, August 20). “Should Companies Track Workers With Monitoring Technology?” Retrieved 1 June
2023, from the Wall Street Journal website:
cy
An anonymous Amazon employee described how human monitors are present to ensure all workers are at least six feet apart and doing their work. While these practices took place during COVID, separating employees using monitors can be counterproductive. There are times when interactions with colleagues would actually enhance productivity, such as if coworkers have questions or require assistance. Communicating with a co-worker would prevent an individual worker from spending valuable time determining an answer when the answer is already readily available. Hiring human monitors and monitoring productivity and performance generally costs resources.

Automated surveillance also leads to work speedups. These work speedups can lead to greater prevalence of on-the-job injury and distress. Workplace injuries and illnesses can also be costly for workplaces. Workplaces may lose productivity due to absence; they may also be responsible for workers’ compensation and medical expenses. Quality control may also become poorer as a result of work speedups, leading to lost revenue, damage to reputation and loss of customer loyalty, increased product recalls, and increased legal fees due to product liability claims, among other concerns.

As opposed to over-invasive, often inaccurate, and discriminatory surveillance methods, we recommend that employers collaborate with their workers on solutions. Workers in the field know best what they need and the issues they are experiencing. Additionally, as U.S. Equal Employment Opportunity Commission (EEOC) Chair Charlotte Burrows noted, “If you’re trying to see if the work is getting done, maybe check that the work is getting done.”

**Part Two: Wage Theft as a Result of Automated Worker Surveillance**

Automated worker surveillance technology leads to wage theft, meaning that workers are unable to receive the compensation they are entitled to under wage and hour laws. Automated worker surveillance technology is used to track worker productivity and activity. Some employers may automatically dock worker pay based on tracked activity. However, this technology is not always accurate or reflective of the actual labor workers exert due to 1) biases in the way these technologies interpret data from subjects who are disabled, marginalized genders, or people of color; 2) biases and incorrect assumptions in the algorithm itself; and 3) technical error.

---

10 See note 2, p. 16.
11 Ibid.
12 See note 1, p. 53.
14 Ibid.
As noted in the next section, the jobs in which these types of technology and practices are most often used are more likely to be filled by women, particularly women of color and disabled women of color. Automated worker surveillance technologies are disproportionately depriving women of their earned wages and subjecting women to unfair labor practices.

Part Three: Discrimination as a Result of Automated Worker Surveillance

Automated worker surveillance systematizes discrimination against marginalized workers. Even if protected characteristics are not explicitly targeted in surveillance or an algorithm, the result is often discriminatory. While automated surveillance technologies might, at first glance, appear “neutral,” the programming and algorithms themselves are not. They are riddled with the biases of the humans that create them, and result in gender, racial, disability and other forms of discrimination as a result.

a. Racial Discrimination

Automated worker surveillance not only leads to racial discrimination, but its roots are based firmly in a history of white supremacy. Automated worker surveillance has an origin in surveillance of enslaved people.¹⁸ Production quotas – and, essentially, this idea of surveillance – were established for enslaved people based on accountings of how much cotton each enslaved person picked per day.¹⁹ Violent punishment ensued for enslaved people who did not meet quotas.²⁰ The value of enslaved peoples was quite literally based on their productivity.²¹ This early implementation of worker surveillance was based in distrust, devaluation, and commodity of Black bodies. Racial stereotypes and disparities pertaining to trust and surveillance continue. People of color and immigrants are concentrated in low-wage jobs,²² and low-wage workers generally are more likely to be surveilled.²³

The primary driver of the wage gap is this “occupational segregation,” which is when women, people of color, disabled people, and those from other marginalized backgrounds are funneled into low-paying, undervalued occupations²⁴ as a result of deliberate policy choices and stereotypes rooted in sexism, racism and ableism.²⁵ The roots of occupational segregation were laid with colonization of Indigenous lands and the establishment of slavery.²⁶ Disabled people were previously sent to institutions, where they were forced to work. Conditions at these institutions were often substandard. With the deinstitutionalization movement came calls for

---

¹⁸ See note 2, p. 7.
¹⁹ Ibid.
²⁰ Ibid.
²¹ Ibid.
²² Ibid., p. 21.
²³ See note 3.
²⁵ Ibid.
community-based care. Even now, not all disabled people receive community-based care, nor do all disabled people have the opportunity to pursue competitive integrated employment in their communities. Subminimum wages and segregated employment are still a reality for many disabled workers. Further, while disabled people are forced into undervalued jobs deemed to be “for disabled people,” disabled women are also forced into undervalued jobs “for women,” compounding the effects of occupational segregation to limit potential earnings.²⁷

Artificial Intelligence (AI) technologies used in automated worker surveillance also pose specific concerns for workers of color. AI technologies using facial recognition have been shown to be less accurate when tracking people of color, particularly women of color.²⁸ Facial recognition technologies have been shown to, quite literally, fail to operate as intended for people of color, even failing to recognize individuals.²⁹

The growing use of automated worker surveillance technologies pose a major barrier to the ability of workers of color, particularly women of color, to participate and advance in the workforce. This barrier is especially pernicious because they specifically target and disadvantage workers of color, particularly women of color workers, while hiding behind the pretext of a seemingly neutral set of data. However, this data is anything but neutral. Data collected to assess and interpret the “productivity” of workers of color, including women of color, may be used in adverse employment decisions, contribute to hostile work environments, and lead to loss and stagnation in income, for example. Employers cannot continue to use invasive data from automated worker surveillance technologies to discriminate against women of color.

b. Disability Discrimination

Automated worker surveillance also contributes to disability discrimination in the workplace. These concerns are even more pronounced for disabled women — particularly disabled women of color. Disabled people, particularly disabled people and women of color, are also more likely to work in lower-wage jobs.³⁰ As noted, low-wage workers generally are more likely to be surveilled.³¹

Time taken to use the bathroom is often considered by employers using automated worker surveillance to determine productivity and performance.³² This is particularly problematic for

³¹ See note 3.
people with disabilities that affect the gastrointestinal or urinary systems, among other chronic illnesses, who might need to take longer or additional bathroom breaks.\textsuperscript{33} Having to share bathroom habits is often beyond the pale of workplace accommodation requests, but when automated worker surveillance is employed that invades a worker’s privacy in such a manner, these types of concerns may arise. In addition to bathroom breaks, the consideration of pauses to rest may also negatively impact disabled workers.\textsuperscript{34} This example was provided in a report published by the Center for Democracy and Technology:

\begin{quote}
\ldots [M]y supervisor was spying on my Outlook calendar schedule and online activity as an administrator who can view all that I can do. I am a sick, disabled, and neurodivergent person. I require breaks in between meetings. When she found out I was taking breaks, she began to micromanage my schedule, my tasks, my time. She also had access as an admin of our advising software that keeps track of advisor-student meetings. \ldots They look at the number of students you are meeting with as a measure of success instead of the quality of interactions. \ldots\textsuperscript{35}
\end{quote}

Finally, a number of disabilities or chronic illnesses can cause some delay in cognitive processing time or physical labor.\textsuperscript{36} Relying on these technologies may lead to punishment of workers for exceeding the average amount of time taken to complete a task, for example.

There is also the concern that these technologies, like with people of color, are simply less accurate when tracking disabled people. Facial recognition technologies are similarly less accurate when it comes to disabled individuals when compared to their non-disabled peers.\textsuperscript{37} Gender and race also play a role in accuracy.\textsuperscript{38} For those who are blind or have other disabilities related to the eye, certain eye movements may also trigger abnormalities for facial recognition and other software, leading to inaccuracy.\textsuperscript{39} Similar concerns arise for autistic workers, workers with ADHD, or workers with other disabilities who may stim.\textsuperscript{40} Additional movement may lead to inaccuracies in tracking. These have also been concerns for students engaged in remote examinations — students may be flagged as cheating simply for having a migraine and looking away from the screen too long, having atypical eye movements (for example, if a test taker is blind), reading a question aloud to help with dyslexia, or stimming.\textsuperscript{41} The same issues are likely to arise in the context of calculating productivity and performance in the workplace.

When employers use aggression detection technology to monitor performance of disabled workers, there are additional concerns. Aggression detection technology, which helps to determine whether there is a present threat, is not designed with disabled people in mind.

\textsuperscript{33} See note 1, p. 53.
\textsuperscript{34} Ibid., pp. 50-51
\textsuperscript{35} Ibid., p. 52
\textsuperscript{36} Ibid., p. 53
\textsuperscript{37} See note 28.
\textsuperscript{38} Ibid.
\textsuperscript{40} Ibid.
\textsuperscript{41} See note 29.
Disabled individuals, such as those who experience tics, such as with Tourette Syndrome; who have cerebral palsy; who are autistic; or who are Deaf or hard of hearing may make noises outside of what is typical. These noises might be misinterpreted by these aggression detection technologies. Dropping items may also be more likely for those with certain physical disabilities, which is also a concern when considering the implications of aggression detection technology.

c. Sex Discrimination

Automated worker surveillance technologies disadvantage women in the workplace, posing an active threat to their job security.

Facial and voice recognition technologies used to collect data pertaining to productivity and performance are less accurate when interpreting data from women, and those who are transgender, non-binary, and of other marginalized genders. Certain types of employers, such as those in retail or customer service, may employ emotional recognition technologies. These AI technologies interpret facial expressions and emotion of a subject. This type of technology is particularly poor at interpreting women’s voices; this issue is especially pronounced for women of color because the technology is not geared toward interpreting their expressions.

With the history of discrimination against women, surveillance and its relationship to privacy is also complex. Women, particularly women with lower incomes and women of color, are more likely to experience harassment and receive unwanted attention in all spheres. These experiences impact feelings pertaining to safety and privacy, understanding that they are more likely to be sexualized or targeted. When women, particularly multi-marginalized women, are surveilled, it adds to this concern, and practice, of placing additional scrutiny and unwanted attention on them.

Pregnancy and pregnancy-related disability discrimination, as well as discrimination against nursing employees, are also a concern. These employees may need to take additional breaks to use the bathroom or to chestfeed or nurse, for example. Automated worker surveillance technology may take these breaks into account without any further consideration. Discrimination based on pregnancy, childbirth, or other related conditions is considered unlawful sex discrimination under Title VII of the Civil Rights Act of 1964, Pregnant Workers Fairness Act and the Providing Urgent Maternal Protections (PUMP) Act. It may also be further protected under state laws.

d. Discrimination against Caregivers

---

42 See note 28.
43 Ibid.
44 See note 3; See note 28.
45 See note 3.
47 Ibid., p. 1080.
Caregiving is foundational to the functioning of human society. Every person born has needed or will need caregiving at some point. This care can take many forms, whether it is caring for one’s child, a parent or grandparent, or a friend or loved one who needs support. For family members, friends, and chosen family, this care may be unpaid. Approximately 53 million Americans provide unpaid care to adults or children with disabilities. In 2021, 40 percent of families lived with their own children.

Sixty-one percent of all caregivers report working while providing care. In half of families with children, women are the primary or co-bread winner. It is therefore not unreasonable or uncommon to assume that caregivers, and women in particular, would be working or rely on income from work in addition to caregiving responsibilities.

Automated worker surveillance technologies pose a particular concern for unpaid caregivers. Unpaid family, friend, chosen family, and other caregivers might need to pause more frequently to attend to children, spouses, parents, or others who need support. That is not an inherent indicator of a lack of productivity or an inability to finish assignments in a timely fashion, and yet it is the type of occurrence that could all too easily cause a worker to be flagged by automated surveillance. These flags can lead to adverse employment decisions and other negative workplace interactions. This bias against caregivers poses particular risks to women workers, workers of color and workers with disabilities, who take on a disproportionate share of caregiving responsibilities.

Women are more likely to take on unpaid caregiving responsibilities. Sixty-one percent of caregivers for adults and disabled children are women, while only 39 percent are men. In 2022, at least one parent was employed in 91.2 percent of households with children. Fifty-five percent

---

54 See note 49, p. 10
of women caregivers report a lack of choice in providing care. All of these caregivers are harmed by the discriminatory implementation of automated worker surveillance.

Racial disparities also exist within our care infrastructure. Asian American, Hispanic, and African American caregivers more often report that recipients of care live in their homes than White caregivers. Additionally, Asian American, Hispanic, and African American children are more likely to provide care than their White counterparts, with Hispanic respondents the most likely to provide care to a parent. Finally, African American caregivers reported providing 31.2 hours of care per week on average, compared to 26 hours of care by Hispanic respondents, 24.1 by Asian American respondents, and 21.2 by White respondents.

Disabled individuals and members of the LGBTQIA+ community are more likely to provide care for chosen family. Leave protections for chosen family are not federally recognized, leaving members of the disabled and LGBTQIA+ and disabled communities to balance work and care for loved ones.

Some jurisdictions, like the District of Columbia for example, also provide protections for workers based on family responsibilities. Use of this automated worker surveillance technology in making any adverse employment decisions may therefore also violate these worker protections.

Discrimination against caregivers in and of itself is an attack on the backbone of our society. However, caregivers also often have intersecting identities, experiencing different aspects of marginalization. Discrimination against unpaid caregivers therefore implicates concerns pertaining to gender, racial, and disability discrimination, as well as discrimination based on sexual orientation, gender identity, and family responsibilities in relevant jurisdictions. For example, Black women have long faced harmful stereotypes about sexuality and motherhood that are deeply rooted in slavery and segregation, and that affect how they are perceived, treated and judged. It is entirely possible, if not likely, that any automated surveillance flags arising from a Black woman’s caregiving responsibilities would be reinforced and exacerbated by these biases and stereotypes, leading to adverse employment decisions, loss or stagnation in income, and unnecessary interference with family and other caregiving responsibilities.

---

57 See note 49, p. 22
58 Ibid., p. 44
59 Ibid., p. 31
61 D.C. Code § 2-1402.11(a)
62 In the District of Columbia specifically, “Family responsibilities” is defined as, “[T]he state of being, or the potential to become, a contributor to the support of a person or persons in a dependent relationship, irrespective of their number, including the state of being the subject of an order of withholding or similar proceedings for the purpose of paying child support or a debt related to child support.” D.C. Code § 2-1401.02(12).
Part Four: Policy Solutions for Addressing Discrimination that Follows Automated Worker Surveillance

For workers to be in the best position to create solutions with employers, strong support of unions, including through legislation and regulations that strengthen worker power, is required. As an important example of the importance of unions in this area, the National Labor Relations Board has held that, when there is a unionized workforce, employers must obtain consent from the union prior to video surveillance of any unit members.\textsuperscript{64} Even without this specific example, unions provide security and support for workers; they also collectively bargain to ensure that concerns like automated worker surveillance are addressed. Unions have been under attack through labor regulations, policy, and case law. Employers understand that weakening unions leaves workers in a position more ripe for exploitation. The Administration’s support of the Protecting the Right to Organize (PRO) Act is critical.

There is also concern that automated worker surveillance can stifle organizing activity. Protected activity may be surveilled, leading to concerns about retaliation or adverse employment decisions. In National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo’s October 31, 2022 memorandum, she discusses this concern in great detail.\textsuperscript{65} We urge that, should such cases arise, the NLRB adopt the framework outlined in Abruzzo’s memorandum, based in well-settled law protecting workers’ rights to organize.

In September 2022, the NLRB proposed a rule establishing a standard to determine when two employers are joint employers.\textsuperscript{66} While we support this proposed rule, we also recommend that the final rule explicitly include use of automated worker surveillance technology in considering evidence of control.

We also recommend public policies that directly address these types of technologies. What data can be collected, how it can be stored, and how and with whom it can be shared are all questions left to be clearly answered.\textsuperscript{67} However, at this stage, employers appear to have very wide discretion. Though courts have found that employers can institute monitoring when the equipment or technology is employer-owned, the employer has a legitimate business interest, or when it occurs during normal working hours,\textsuperscript{68} this language is quite broad. The only major federal law that addresses monitoring directly is the Electronic Communications Privacy Act of

\textsuperscript{67} See note 2, p. 4.
\textsuperscript{68} Ibid., p. 29.
1986.\(^69\) Under this Act, oral and written employee communications may be monitored if there is a legitimate business purpose.\(^70\) However, the ECPA is quite outdated. Regulatory and statutory updates that better reflect the way data is used and stored are needed.

Additionally, protections for workers are not necessarily consistent across states. For example, several states have statutes that require employers to provide employees with notice of surveillance. This Administration’s support of legislative policies that provide employees with notice and additional protections related to automated worker surveillance, in addition to clear prohibitions on and guidance for employer use, would be a pivotal step to ensuring that all workers are free from discrimination, regardless of where they live or work.

Even given the limited number of federal laws that directly address automated worker surveillance, administrative action is possible under several different avenues. First, under Occupational Safety & Health Administration’s (OSHA) own directives, it can adopt standards requiring employers to curb the harmful effects of automated surveillance technologies.\(^71\) Meanwhile, the National Institute for Occupational Safety & Health (NIOSH) may conduct research on the effects of automated worker surveillance on worker health.\(^72\)

While the above proposals appear to be neutrally tailored, marginalized workers experiencing discrimination and harm as a result of the use of these technologies would most benefit from the implementation of these proposals. However, there are also policy solutions that can directly address the discrimination that marginalized workers experience.

The U.S. Equal Employment Opportunity Commission (EEOC) should establish regulations or guidance under federal anti-discrimination laws, including the Americans with Disabilities Act (ADA) and Title VII of the Civil Rights Act of 1964, that clarify what constitutes discrimination when automatic surveillance technologies are in use. This work would be consistent with the EEOC’s current Artificial Intelligence (AI) and Algorithmic Fairness Initiative.\(^73\) The EEOC has already issued guidance around how employer use of software, algorithms and AI in employee assessment and hiring practices must comply with the ADA.\(^74\) It has also published technical assistance on the ways that employers can run afoul of Title VII of the Civil Rights Act of 1964 using these technologies and algorithmic decision-making.\(^75\) The EEOC can build upon this


\(^70\) 18 U.S.C. § 2511(2)(a) (2022); See note 64.

\(^71\) See note 1, p. 56.

\(^72\) Ibid.


guidance and technical assistance by issuing further guidance specifically on employee assessment through automated worker surveillance. Additionally, the EEOC should prioritize enforcement against employment discrimination aided by automated worker surveillance and other forms of AI.

The U.S. Department of Labor’s Office of Federal Contract Compliance Programs (OFCCP), through its work holding federal government contracts and subcontractors responsible for violations of anti-discrimination laws, should also prioritize enforcement against employment discrimination aided by automated worker surveillance and other forms of AI. OFCCP may also wish to publish guidance and regulations about the types of evidence it may consider when pursuing this enforcement.

Conclusion

The National Partnership for Women & Families urges the federal government to consider and implement the above-described recommendations with regard to automated worker surveillance technologies.

Thank you for your consideration of the National Partnership’s comments to this RFI. If you have any questions about this comment, please contact Marissa Ditkowsky, Policy Counsel for Disability Economic Justice at the National Partnership for Women & Families, at
The UC Berkeley Labor Center welcomes the opportunity to provide input to the White House Office of Science and Technology Policy (OSTP) in response to the Request for Information on Automated Worker Surveillance and Management posted on May 1, 2023.

The mission of the Labor Center’s Technology and Work Program is to provide worker organizations and policymakers the research and policy analysis they need to respond to rapid technological changes in the workplace and ensure that technology benefits rather than harms workers. We focus on low wage industries and the workers of color, women, and immigrants who are often on the frontlines of experimentation with emerging technologies.

We are very pleased to see the White House Office of Science and Technology Policy’s attention to automated workplace surveillance and management technologies and interest in exploring opportunities for Federal agencies to ensure that these systems do not harm workers and undermine their rights and
opportunities.

Drawing from our own research analyzing trends in the data-driven workplace and impact of these technologies on workers, our goal in this comment is to highlight that the workplace is rapidly becoming a major site for the use of AI-based technologies, and that workers are therefore a critical constituency in the discussion about AI governance. As an addendum, we highlight evidence indicating the prevalence of automated workplace surveillance and management technologies (Section I), impact on workers resulting from employers’ use of these systems (Section II), and principles and policy models for worker technology rights and protections (Section III) and submit our research publications which analyze trends in the data-driven workplace and provide a comprehensive framework of the technology rights that workers need and deserve.

Thank you for the opportunity to provide these comments.

Annette Bernhardt, PhD
Director
Technology & Work Program

Lisa Kresge
Lead Researcher
Technology & Work Program

Kung Feng
Policy Researcher
Technology & Work Program

Attachments:
Full Comments: UC Berkeley Labor Center Response on Automated Worker Surveillance and Management
Report: Technological change in five industries: Threats to jobs, wages, and working conditions

Attachments
Attachment1_UC Berkeley Labor Center OSTP Full Response
Attachment2_Data and Algorithms at Work
Attachment3_How common is employers use of workplace management technologies
Attachment4_Technological change in five industries
TECHNOLOGICAL CHANGE IN FIVE INDUSTRIES: THREATS TO JOBS, WAGES, AND WORKING CONDITIONS

Jessie HF Hammerling, Ph.D.
UC Berkeley Labor Center
Acknowledgments

The UC Berkeley Labor Center and Working Partnerships USA commissioned the original research discussed in this piece. Funding for that project was provided by the Ford Foundation, the Open Society Foundations, the SEIU California State Council, the W.K. Kellogg Foundation, the David M. and Abby Joseph Cohen Summer Research Fund, and the Cornell University ILR School “Technology and the Future of Work” theme project. Special thanks to Annette Bernhardt for her leadership throughout the project, and her thoughtful input and review of this report. I’d also like to thank the reviewers for sharing insights and feedback: Chris Benner, Jeffrey Buchanan, Françoise Carré, Beth Gutelius, Sara Hinkley, Ken Jacobs, Lisa Kresge, Adam Seth Litwin, Jenifer MacGillvary, Chris Tilly, and Steve Viscelli. Please address correspondence to the author at jesshf@berkeley.edu. Any errors are the responsibility of the author.

Cover design by Sandy Olgeirson.

About the Author

Jessie HF Hammerling is the co-director of the Green Economy program at the Labor Center. Her work examines the impacts of climate change and clean energy policy on workers and communities. She works in collaboration with government, industry, unions, and community stakeholders to develop strategies for fighting climate change that lead to quality jobs and equitable outcomes. In prior years, Dr. Hammerling worked with the Labor Center’s Technology and Work program, where she led research on how employers are using new technologies in the workplace, and developed new training for unions on these topics. Other areas of work have included research on outsourcing, financialization, and food systems. Prior to joining the Labor Center, she worked at the Center on Wisconsin Strategy (COWS) in Madison, Wisconsin. Dr. Hammerling holds a Ph.D. in geography from UC Davis and a master’s degree in international public affairs from the University of Wisconsin-Madison.

Suggested Citation

Introduction

Workers in the U.S. were facing many questions about their future prior to the onset of the COVID-19 pandemic, and that uncertainty has only intensified as the pandemic lingers, and employers’ use of new technologies continues to evolve. Policymakers, worker advocates, and researchers are watching and evaluating which technologies employers are choosing to adopt, and what consequences these changes might have for workers’ jobs. Understanding how technological changes may unfold in different industries is essential for developing effective solutions to the challenges that workers face.

From 2018 to 2020, the UC Berkeley Labor Center and Working Partnerships USA brought together a team of experts to investigate trends in several industries in the U.S. that have been focal points for these concerns: trucking, warehouses, health care, retail, and food delivery. Our team of researchers conducted multi-year studies of each industry, examining how new technologies are changing work and why, what new technologies are on the horizon, and what factors are shaping job outcomes.¹

The intent of the industry studies was not to predict the future or to develop a broad, unified theory of technological change. Instead, the objective was to examine how and why technological change is unfolding in key industries and assess what these changes could mean for different groups of workers. While many of the important findings from these studies are industry-specific, some common themes emerge across the research. In this report, we synthesize the findings of the industry studies, and discuss what they suggest about how policymakers and industry stakeholders should approach the challenges and opportunities workers face in a changing technological landscape.

One of the most striking findings from these studies is that technology’s effects on job quality—like wages and working conditions—should be just as big of a concern as its effects on job quantity. Employers’ use of automating technologies could lead to job loss for specific occupations, but this is just one of many ways that technological change threatens workers’ livelihoods. Rather than replacing large numbers of workers with
robots, our researchers find that employers are using technology to change how workers do their jobs: how they are hired; what tasks they are asked to do, how many and how quickly, and how they are instructed to do them; and how their performance is monitored and assessed. Sometimes technology-related changes are helpful to workers—enhancing their skills or safety, for instance—but far more often they are harmful to wages and working conditions. Technological changes can also worsen existing inequities for women and people of color, who are overrepresented in the many front-line occupations that are most likely to be changed by technology.

The introduction of new technology in low-wage industries can easily lead to bad outcomes for workers, but this is not inevitable. Our studies identify important sources of variation in how technological change happens across and within industries, and multiple scenarios for future adoption. These findings suggest that how and why employers implement new technologies in the workplace is not predetermined. The choices we make now and the regulations we implement can re-shape the course of technological change and its consequences for the U.S. labor market.

The five industry studies

- **DRIVERLESS? Autonomous Trucks and the Future of the American Trucker**
  by Steve Viscelli (September 2018)

- **The Future of Warehouse Work: Technological Change in the U.S. Logistics Industry**
  by Beth Gutelius and Nik Theodore (October 2019)

- **Technological Change in Health Care Delivery: Its Drivers and Consequences for Work and Workers**
  by Adam Seth Litwin (June 2020)

- **Change and Uncertainty, not Apocalypse: Technological Change and Store-Based Retail**
  by Françoise Carré and Chris Tilly, with Chris Benner and Sarah Mason (September 2020)

- **Delivering Insecurity: E-commerce and the Future of Work in Food Retail**
  by Chris Benner and Sarah Mason, with Françoise Carré and Chris Tilly (December 2020)
Findings

1. Employers’ use of new technologies is changing the content of workers’ jobs, but is likely to have limited effects on the overall number of jobs

Each team of researchers identified various new technologies that employers are using in each industry. These ranged from relatively simple improvements in internet and communications technology and digitization of information to complex data collection and algorithmic technologies, including but not limited to autonomous machines. Across the industries we studied, our researchers found that employers’ use of new technologies is altering both the content and the processes involved in people’s jobs in a range of ways.

Employers’ use of new technologies may cause job reductions in some specific occupations, but is not expected to lead to an overall reduction in the number of jobs in the industries studied.

Our researchers found that technology-induced job loss is a real concern for specific occupations. Most notably, nearly 294,000 long-haul truck drivers are at risk of losing their jobs in coming years due to advances in automated driving technologies. Retail and grocery employers are likely to continue thinning the ranks of cashiers by shifting check-out work to customers through self-check-out stations or app-based check-out. In addition, advances in productivity tracking and managerial technology may lead to reductions in supervisors and secondary managers in larger stores. In hospitals, semi-autonomous service robots could reduce the overall number of people employed as orderlies, dietary clerks, and laundry workers; COVID-19 may have jump-started this trend, as hospitals have looked for ways to limit human interactions to reduce the risk of transmission.

Across industries, however, our researchers did not find that widespread technology-induced job loss was currently happening, or that it was likely to happen. In some cases, a growing
demand for services—due to changing consumer preferences (e.g., e-commerce) or changing demographics (e.g., an aging population requiring more healthcare services)—has led to a demand for more workers. In these circumstances, overall demand for certain occupations of workers is outpacing technology-induced job loss or slower job growth. Other factors contributing to worker shortages in specific industries—such as long-term wage stagnation for truck drivers—may result in labor demand for workers continuing to outpace supply, even as automation reduces the overall number of jobs.5

Furthermore, the pace of technology adoption is often slower than expected and uneven within industries. Despite abundant speculation about the possibility of highly-automated “dark warehouses” and a “retail apocalypse” due to the growth of e-commerce, neither of these scenarios appears probable any time soon, according to our researchers.6 In trucking, employers are unlikely to transition from human drivers to broad reliance on automated driving technology for delivery in the near future, despite the real possibility that they will implement these changes in some form for long-haul trucking.7

Another reason that large-scale job displacement is unlikely in the foreseeable future is that the technology to automate certain types of tasks, such as item-picking to package e-commerce orders or delivery vehicles navigating complex urban environments, remains inadequate for employers’ needs. And even where technology exists that is capable of automating certain tasks, there may be other reasons employers prefer a person to a machine in a particular role. For instance, employers may prefer a human worker to answer a customer’s questions about a product in a store, or to identify an appropriate place to leave a package at someone’s residence.

New technology can also be prohibitively expensive, especially in highly cost-sensitive industries. In warehousing, slim profit margins and cost-based competition have led to a cautious approach to new technology.8 The growth of e-commerce has spurred experimentation with new technologies among industry leaders like Amazon, but many other firms still lag far behind in adopting even simple technologies like digital warehouse management systems.9 Similarly, a “digital divide” exists in retail, where market leaders—especially those who have effective channels for participating in e-commerce—have the resources to invest in the latest technology, while other smaller firms do not.10

Despite abundant speculation about the possibility of highly-automated “dark warehouses” and a “retail apocalypse” due to the growth of e-commerce, neither of these scenarios appears probable any time soon.
Employers are using technologies in ways that create new tasks and jobs, and shift the allocation of tasks across machines, workers, firms, and customers.

Understanding how new technologies are changing some workers’ jobs requires an examination of the ways in which technologies affect the specific tasks the jobs involve. Every occupation consists of an assemblage of tasks, which often vary across industries or employers, and can change for all kinds of reasons, including employers’ adoption of new technologies.

Some tasks are easier than others to execute using technology, such as those that involve highly structured and repetitive actions. Even so, employers rarely use technologies to replace all tasks involved in a worker’s job; technologies are more often used to substitute for specific tasks, leaving other aspects of the job intact but potentially transformed. For example, where employers use automated chatbots to field customer service calls, human representatives may end up fielding more complicated inquiries, while the simpler ones are resolved by machines.

Technology-enabled task reorganization can create new tasks, such as remote operation of semi-autonomous vehicles, maintenance and programming of new machinery and software, and managing and staffing order-picking and curbside pickup for retail and grocery stores. This may create new jobs, increase the demand for certain jobs, or change the scope of work involved in a job.

In some cases, technologies are used to transfer tasks between customers and workers. In a customer self-checkout system, the core tasks of a cashier—ringing up and bagging groceries—are not automated but transferred from a worker to a customer. On the other hand, online ordering for groceries transfers tasks that customers would otherwise do—such as filling a cart and taking the food home—to workers.

Employers may also use technologies in ways that redistribute tasks among different workers. These could be workers within a particular firm, or workers employed in other firms, or independent contractors. In some grocery stores, retrieving and packing groceries for online orders is carried out by employees of the store, but in other cases (and sometimes within the same store) these tasks are carried out by a worker employed or contracted by a third party, such as Instacart. Similarly, restaurant take-out deliveries may be completed by restaurant employees, or by workers affiliated with a third-party ordering platform like Doordash or UberEats.
Employers’ use of technologies may contribute to broader shifts in employment as well, across industries or market segments. The increased reliance on e-commerce for retail sales, for instance, has reduced demand for employment in stores, but increased the need for workers in warehouses and trucking. It has also shifted unpaid work by consumers in shopping and driving to paid work in order fulfillment and home delivery services.

**Employers are using technologies in ways that change how job tasks are done.**

In addition to the reshuffling of tasks, employers are using new technologies in ways that change the processes involved in workers’ job tasks. Advances in data collection and algorithmic technologies are enabling employers to make changes to a broad array of HR and management functions, such as hiring, scheduling, task direction and pacing, monitoring, evaluation, and discipline or dismissal. These changes serve specific functions; here, we describe several types of managerial objectives, offer examples of the technologies that employers are using toward those ends, and discuss how these technologies change the way workers complete their tasks.

**Safety:** Some employers are using technologies intended to make work safer; examples include machinery that can alleviate the need for heavy lifting and sensors that track driving conditions, vehicle operations and potential safety hazards. These technologies can change the physical processes involved in workers’ tasks, or give workers real time notifications to adjust their actions.

**Personnel decision-making:** In some cases, employers use data-gathering and analytic processing software to compile and interpret information about current or prospective employees, which human managers then take into consideration in their decisions about personnel. In other cases, employers are using algorithmic technologies to replace certain aspects of human decision-making altogether.

**Information-sharing:** Employers in many industries are using technologies that can facilitate communication and information-sharing, which can affect work processes in a wide variety of ways, such as changing the order in which workers complete their tasks, and giving them real-time direction and feedback. A few of the far-reaching range of examples of these types of technologies include delivery apps, customer service platforms, telehealth, and electronic health records.

**Pace-setting:** In several of the industries our researchers studied, employers are using technologies aimed at speeding up work processes to reduce costs. For instance, warehouses and retail stores may use digital inventory tracking systems and stocking devices to help streamline workers’ movement of goods in a facility. Delivery drivers often use mapping and route-planning software intended to optimize speed and maximize their number of deliveries.
Monitoring: Employers are also using technologies to monitor and track workers’ locations, activities, and the accuracy of their work. This type of tech is increasingly common in warehouses and delivery, but is also being deployed in home health care, where employers are using phone-based software to manage workers remotely by tracking their location and task-completion at clients’ residences.

The managerial objectives highlighted here are not exhaustive, nor are they mutually exclusive. Employers adopt technologies and make other changes to production processes for a complex array of reasons. These changes can affect the processes involved in workers’ jobs in intended and unintended ways, and can have both positive and negative effects on job quality. In the next section, we discuss the consequences of employers’ use of new technologies for workers.

2. Employers in each industry are using new technologies in ways that may degrade workers’ wages and working conditions and worsen existing labor market inequities

Employers can use new technologies in ways that are helpful to workers, as some of the above examples indicate. Technologies can make work safer, and reduce worker time spent on paperwork or arduous, repetitive tasks. However, in each industry, our researchers concluded that many employers are likely to use new technologies in ways that threaten workers’ wages and job quality.

Employers’ use of technology to reorganize work and production could lead to lower wages, deskilling, and deteriorating job quality for workers.

When employers reorganize and reshape production processes, the changes they make can have consequences for workers’ wages and job quality. While the consequences aren’t invariably or inevitably negative, our researchers found that technologically-induced task redistribution may result in poor outcomes for many workers.

When employers use technology to reshuffle tasks among workers within the firm, workers may see a reduction in the range or complexity of tasks involved in their work, which employers can use as justification for lower pay. In some cases, workers may actually experience a pay cut following technologically-induced reorganization of work processes; in others, an industry may experience a longer-term shift toward lower pay for certain occupations. In health care, chatbots and autonomous service robots are starting to be used in ways that reduce staffing
Employers’ use of technology to redistribute tasks to workers outside of the firm also can have negative implications for workers’ wages and job quality. In retail, restaurants, and grocery, employers are using technology to reallocate tasks (e.g., delivery or shopping, as discussed above) to workers employed by third-party firms or hired as independent contractors. In warehouses, employers are turning to on-demand staffing platforms to hire temporary workers through staffing agencies, in some cases via third-party logistics (3PL) management firms. Regardless of the industry, workers employed by third-party firms are likely to be paid less and lack access to benefits that workers at the lead firm may have, including union representation. Workers hired as independent contractors lack access to basic employment rights and legal protections, such the right to a minimum wage, collective bargaining, and workers’ compensation in case of injury.

Technologically-induced reorganization of production processes has also resulted in work being shifted within industries in ways that favor lower-wage segments. In trucking, the jobs most at risk of displacement from automation are long-distance truck driving jobs, which have higher rates of pay compared to local delivery jobs; the latter increased in number as e-commerce has grown but are much harder to automate.

Employers’ use of technology to change work processes can lead to work speed-up accompanied by decreased autonomy and privacy for workers.

Employers are using new technologies in ways that can impinge on workers’ autonomy and privacy, and that speed up and intensify their work. Amazon has been a leader in the development and adoption of technologies that increase employers’ surveillance and control over workers. At Amazon warehouses, workers are closely monitored using video surveillance, and tools like GPS-enabled handheld devices and wearable tech embedded with sensors. These devices gather and record data on workers’ location and activities, which are used not only for general monitoring but also as inputs into algorithms that direct workers’ tasks. Besides setting the pace of work, the algorithmic systems are used to assess workers’ performance and speed. Workers’ time spent “off-task,” including time spent walking to and from a restroom or break room, is automatically recorded. If the workers aren’t meeting specific productivity targets, they are penalized and may be fired.
The intensive surveillance and grueling pace at Amazon warehouses have been well-documented in media accounts and have been cited as an important impetus to attempts to organize warehouse workers into unions. Workers report that the conditions in Amazon warehouses take a serious mental and physical toll, leading to exhaustion, workplace injuries, and psychological stress induced by the pressure to achieve their required productivity rates. Warehouse workers are far from the only workers who have experienced negative consequences from employers’ use of new technologies that reshape work processes. Electronic visit verification (EVV), a software which allows home care workers to be managed and monitored through a smartphone by tracking their location and activities in real-time, is an increasingly common technology in home health care. The use of EVV has created an environment where many workers report feeling increased stress from micromanagement, constant surveillance, and invasion of their privacy.

In trucking, drivers can be exposed to an extreme amount of data collection and electronic monitoring. Employers use sensors and real-time visual data streams to track and assess everything happening inside or around the vehicle, including location, possible hazards, driving patterns (speed, acceleration, braking, etc.), and driver behavior (seatbelt use, driver fatigue, or other distractions like texting or eating). Fleet managers can use these systems to “exert control over workers by setting quantified metrics to evaluate driver performance and challenge workers’ accounts of driving conditions.”

Major retailers frequently use algorithmic technologies as part of their processes for hiring, scheduling, and managing workers. Stores are using cameras and other sensors to track and monitor product inventory and store conditions, meaning that clerks and stockers can receive real-time alerts and direction about where and what to restock, or where to clean. Delivery drivers and in-store shoppers (e.g. for Instacart) can be tracked and directed by employers and/or customers in real time via apps that monitor location and item selection. These workers have reported that constant location tracking and other forms of electronic monitoring, plus algorithm-generated metrics that intensify workload and time pressure, have added to the mental and physical stress of their jobs and increased the potential for accidents and injuries.

**Employers are using new technologies in ways that can worsen existing labor market inequities.**

The peril arising from employers’ use of new technologies is not borne equally across all workers. Many of the occupations facing significant threats from technologies that displace, monitor, control, and speed up work are those in which higher concentrations of women and people of color are employed. In warehouses, people of color are overrepresented compared to the labor market at large, and women are a growing portion of the e-commerce warehouse sub-sector. In retail and grocery, women are more likely than men to work in customer-facing
roles like cashier, which will continue to decline in number as employers turn to self-checkout and e-commerce. Women are also overrepresented in most health care occupations (apart from the highest-paid positions like physicians and surgeons), and Black and Latino workers are concentrated in the lowest-paid jobs like home health aids, which are increasingly subjected to surveillance and monitoring technologies.

Certain new technologies have biased outcomes for women, people of color, and other disadvantaged workers. For example, productivity-based pay structures to incentivize speed in warehouse work creates additional challenges for workers who are not as strong or physically fit, such as older workers. Additionally, algorithms used in applicant screening and hiring processes are notorious for replicating and exacerbating existing patterns of discrimination in the labor market. Research also indicates that technologies like speech and facial recognition can be less accurate in identifying and communicating with women, people of color, and people whose first language is not English. This can create additional barriers for workers who must interact with these systems in their jobs.

The work of our researchers and others suggests that the most serious repercussions of new technologies in the workplace will fall on those workers already facing the greatest structural challenges in the labor market. The use of new technologies will worsen existing inequities.

3. **Industry context shapes employer decision-making about new technologies, leading to variation in adoption and worker impacts**

A defining feature of each of our researchers’ projects was the recognition that industry context shapes technology adoption decisions. Across and within industries, our researchers observed variation in the pace of employers’ uptake of new technologies, their goals with respect to technology, and the consequences of these changes for workers. The factors that had the biggest impact on technology adoption fell into five categories: regulations, worker organizations, competitive structures, industry trends, and broader societal and market trends. These factors shaped employers’ understanding of how they might use new technologies in the context of their other objectives and priorities. In some cases, these factors accelerated technological adoption and in others they hindered it.
Regulations

Regulations establish the ground rules that shape competitive market strategies, distinct market segments, and the distribution of power across market actors. Variation in regulation by industry or by region therefore plays a formative role in shaping employers’ technology adoption decisions.

Each industry is governed by a unique set of laws and regulations that are subject to change over time at the discretion of policymakers. These changes affect the context guiding employer decision-making, and can have direct and indirect effects on technology adoption and working conditions. For example, long-term deregulation over certain aspects of the trucking industry has weakened workers’ power relative to employers, and reduced job quality and working conditions for many truck drivers. These changes have created distinct labor markets in trucking where workers are especially vulnerable to the invasive or exploitative effects of employers’ adoption of new technologies. For instance, in local delivery and port trucking, independent contractor misclassification has proliferated and worker protections are minimal. As we have noted, local delivery tasks remain highly reliant on human workers; as a result, local delivery firms are more likely to invest in technology that monitors and controls workers rather than attempting to replace them, and drivers have limited means to object.

The health care industry, on the other hand, is highly regulated. Health care involves a complex web of actors and regulations, organized around a division between the providers of care (hospitals, etc.) and the financers of care (insurance companies and the government). In recent years, the government has tried to guide the market toward payment models based on “value-based care” (VBC) rather than “fee for service” care, which increase quality and efficiency of care provision. Under VBC models, insurers contract to reimburse providers on a fixed rate (e.g. per-member-per-month), so providers internalize the risk of variable costs associated with their patient population, and thus they no longer have an incentive to maximize the number of claims submitted to insurers.

The shift toward VBC is likely to accelerate the adoption and diffusion of quality-enhancing health care technologies, such as those that facilitate patient-provider communication and increase access to preventative care. Regulations advancing VBC may be a promising shift for the health care industry for many reasons, but the constraints that VBC places on health care providers’ income can also pose challenges for workers’ bargaining power by limiting the overall amount of resources.
available for wages and benefits. Ensuring that workers are not penalized by the shift to VBC will require additional regulation and worker organizing.42

Broader regulations influence markets and technology adoption across industries. In many areas of regulation in the U.S., laws and policies favor the rights and freedoms of employers relative to workers, which creates incentives for employers to compete on labor cost cutting strategies.43 Weak federal labor laws have limited the power of labor market institutions like unions to bargain for better wages and working conditions—including working conditions related to technology.44

Some states have stronger labor regulations, however, such as laws that specifically target independent contractor misclassification. Other states have laws that make it more difficult for workers to advocate for their rights and form unions. Twenty-eight states have “right to work” (RTW) laws that inhibit worker organizing. In RTW states, labor unions have less power to shape legislation or working conditions, and wages for workers tend to be lower.45 The strength or weakness of labor regulation affects workplace technology deployment in important ways; workers’ ability to fully participate in this process can be inhibited or enhanced depending on the law, as can their ability to organize to protect themselves from potential harms of new technologies (see next section).

The lack of regulation governing employers’ uses of technology in the workplace has had a profound effect on employers’ use of technology in relation to their workers. As we note in our 2021 report *Data and Algorithms at Work: The Case for Worker Technology Rights*, the dearth of regulation creates strong incentives for employers to use digital technologies widely, and in ways that can directly or indirectly harm workers. There is also no oversight of the testing and quality of new systems that developers sell, which can worsen adverse effects for workers.46

Recent efforts to remedy this challenge have been promising, however. In September 2021, California passed a bill targeting the grueling pace of work in Amazon warehouses by limiting companies’ use of production quotas, and improving transparency around the use of algorithms in setting quotas, and several states have since passed or proposed similar legislation.47 In April 2022, California legislators introduced A.B. 1651, The Workplace Technology Accountability Act, which would establish broad protections for workers against employers’ use of monitoring and algorithmic management technologies.48 Legislators in California and elsewhere have passed laws fighting independent contractor misclassification, granting employment protections like minimum wage, overtime, and workers’ compensation to workers in trucking and app-based delivery.49
Worker organizations

Unions and worker organizations can affect technology adoption patterns in individual firms, and in the industries and regions where they represent significant portions of an industry’s workforce. Health care workers are more likely to be represented by a union than workers in many other industries in the U.S. This affords them more power in influencing employers’ decisions related to technology. For example, at Kaiser Permanente, unions played an important role in facilitating the company’s switch to an Electronic Health Records system, ensuring effective deployment and use of the system, and protecting employment and wages for workers affected by the new system.

Unions also play an important role in certain segments of the trucking and grocery industries. The most recent contract negotiated between United Parcel Service (UPS) and the Teamsters union includes a requirement that UPS give the Teamsters six months’ notice of any company plans to integrate emerging tech, such as drones, driverless vehicles, or truck platooning. The United Food and Commercial Workers union (UFCW), which represents grocery workers, has fought to keep the growing numbers of e-commerce and delivery jobs in-house. UFCW has challenged employer attempts to outsource these jobs to third-party app-based shopping companies that typically use non-union workers or independent contractors.

Worker organizations can also affect technology adoption by attempting to create policy. Where unions do not currently exist in significant numbers, other organizations representing workers—such as United for Respect in the retail sector, the Warehouse Workers Resource Center, and Gig Workers Rising—have been leading efforts to advocate for stronger regulations of industries around technology and other job quality issues. In some cases, worker organizations have partnered or allied themselves with unions.

Competitive structures

Regulations create a unique structure of competitive and cooperative arrangements between firms in each industry. Market structures and market power shape employers’ strategies for growth and survival: what problems are employers trying to solve, what technologies could address those problems, and what factors will affect an employer’s decision to invest?

Weak antitrust enforcement in the U.S. has allowed ownership consolidation to proliferate in many industries, which in turn has led to a gap between large, well-resourced industry leaders that are able to invest in and experiment with cutting-edge technologies, and smaller firms that tend to lag far behind. This dynamic is especially notable in retail and warehouses. Historically, employers in both industries have been slow to adopt new technologies. The rise of Amazon has reoriented the competitive terrain in both sectors, however, compelling other large employers to integrate new technologies related to e-commerce ordering and delivery into their business strategies, while smaller firms continue to take a more cautious approach.
The market dominance of a firm like Amazon means that it has an outsize influence on the competitive landscape of an industry, including on employer objectives regarding technology. Firms with the means to invest are focused on technologies that can promote speed in processing, packaging, delivery, and cost-reduction at every step of the way. Large retailers are also concerned with strategies to increase their own market share and to develop new revenue streams. For some smaller retailers, however, growing consumer expectations about low-cost, rapid online ordering and delivery options are reducing their ability to attract customers, further constricting resources available to adopt new technologies.\(^{56}\)

In industries where ownership consolidation is less extreme, employers still face similar pressures to reduce wages, speed up work, and micromanage their workers, but a wider range of strategies related to technology adoption can exist. In the grocery and trucking industries, for instance, there are major employers with unionized employees. At unionized firms, workers can exercise their collective market power to influence the effects of new technologies on their jobs, as in the examples discussed above.

In health care, the government is the dominant market actor. Although most people in the U.S. have private insurance through their employers, the U.S. government funds Medicare and Medicaid, making it the largest single buyer of insurance in the U.S. As such, it has significant leverage and buying power in the industry. Thus, when President Obama signed the 21st Century Cures Act, which required home care agencies that provide personal care services to have EVV technologies or risk losing their Medicaid claims, “the federal government essentially ‘picked a winner,’” ensuring that this type of technology would proliferate across the market for home care.\(^{57}\)

**Industry trends**

Ownership consolidation is not the only industry trend creating distinct patterns of technological change. As another important example, changes in consumer preferences also have a profound effect on patterns of technology adoption in each industry. The increase in e-commerce has reoriented employer objectives across several of the industries we studied, including retail, grocery, warehouses, and trucking. Developing effective platforms for online shopping is of course a priority for many employers, as is deploying a wide range of technologies to facilitate rapid order assembly and delivery. Similarly, growing consumer demand for prepared or semi-prepared food rather than groceries has put pressure on traditional grocery stores to...
develop more options in this area. One result is that some grocery stores are partnering with subscription-based meal kit companies, which typically rely on warehouse-like facilities where workers’ wages and job quality are comparatively low.\textsuperscript{58}

In the warehouse industry, there are important differences between production processes for shipping in e-commerce facilities and traditional warehouses. Processing in traditional facilities involving bulk transfer of products is far less labor-intensive and time-sensitive compared to processing in e-commerce facilities. As a result, traditional warehouse employers may be less interested in the kind of intensive employee surveillance pioneered by Amazon, and more interested in advances in warehouse management systems and machinery to automate movement of goods around a facility.\textsuperscript{59}

Another industry trend affecting technological adoption is outsourcing. We’ve already discussed outsourcing in the context of trucking, grocery, and food delivery, and the implications of these changes for workers, in particular independent contractors, who lack basic employee rights and protections on the job. There has also been an increase in recent years in firm-to-firm outsourcing in some sectors, such as retailers outsourcing warehouse services to third-party logistics companies (“3PLs”). Competition in the 3PL market is extremely price-sensitive, and contracts are often short-term, which may blunt employers’ incentives to invest in specialized technology.\textsuperscript{60}

**Broader societal and market trends**

The COVID-19 pandemic, long-term demographic changes, and shifts in economic conditions and labor markets all affect patterns of technological change across multiple industries, but the consequences of these trends are not uniform across or even within industries. In particular, the pandemic appears to be speeding up technology adoption in some cases but slowing it down in others. For example, grocery employers have rapidly shifted to online ordering and health care providers to telehealth options since 2020; these are both technologies that had made limited inroads prior to the pandemic. On the other hand, financial constraints in stores and restaurants caused by declines in in-store shopping and eating have limited some employers’ ability to experiment or invest in any new technologies.\textsuperscript{61}

COVID-19 has also reshaped employers’ objectives and strategies related to technology. In industries where workers have been required to work onsite, such as health care, grocery stores,
and warehouses, technologies that could help reduce disease transmission for customers or workers became a priority for some employers.\textsuperscript{62} These included new forms of data gathering on workers’ health to prevent and track outbreaks, and technologies that reduce the need for on-site workers or reduce their physical proximity to one another, such as semi-autonomous service robots and cashierless checkout.\textsuperscript{63}

Societal and demographic trends affect industries’ uptake of technology as well. Women’s long-term increases in labor force participation has induced growing demand for prepared food along with online ordering of groceries and takeout. In the U.S., people are also living longer on average, which creates an interest among health care providers in technologies that can respond to the increasing demand for long-term care.\textsuperscript{64} Additionally, an aging workforce has led to a retirement bubble in certain industries that may exacerbate ongoing labor shortages, with a prime example being trucking.

Broader trends may work in favor of or against workers in terms of technology adoption and its consequences. Labor shortages are benefiting some workers in sectors like trucking and warehousing by prompting long-overdue wage increases, but they may also accentuate employers’ interest in technologies that reduce employers’ reliance on workers in the long-run.\textsuperscript{65} As discussed above, the pandemic has likely accelerated some employers’ interest in labor-displacing technologies and employee surveillance technologies, but it has also reduced some employers’ ability to invest in such technologies, potentially slowing the pace of change in certain industries and market segments.
Conclusions

Recent technological advances such as big data, robotics, and artificial intelligence have expanded our technological capabilities exponentially, and are poised to accelerate the pace of change in many industries. In some cases, employers will deploy new technologies in ways that reduce the number of jobs available. In other cases, they will use new technologies in ways that expand the numbers of existing jobs or create entirely new types of positions. Employers also will continue to use new technologies to reorganize production, reshuffle tasks, and change work processes. Across all the industries our researchers studied, we found that new technologies pose a significant threat to workers’ wages and job quality, and equity for women, people of color, and other disadvantaged workers. Many employers are using—or exploring the use of—technologies that facilitate monitoring and control over workers’ actions, speed up the pace of work, and generally devalue workers and their contributions.

The COVID-19 pandemic has injected additional uncertainty into forecasting the future of work; it serves as an important reminder that the form new technologies take and the consequences they have are not preordained. What the jobs of tomorrow will look like depends on the choices we make now to shape the course of tech development and adoption, and on the mitigable ground rules for the economy overall and for the industries in which these decisions are situated. Our studies illustrate how employers’ choices about technological change occur within the context of specific industries and markets, and the regulations and institutions that guide and govern how firms function.

The same forces that have constrained workers’ ability to improve their wages and working conditions are currently on course to wield disproportionate influence over the types of technologies that are developed and the ways they are deployed in each industry.

The same forces that have constrained workers’ ability to improve their wages and working conditions are currently on course to wield disproportionate influence over the types of technologies that are developed and the ways they are deployed in each industry.
our industry studies we have highlighted the importance of regulations to allow workers to help shape the process of technological change, and for employers to be motivated to make choices that prioritize quality-based over cost-based competition. Industry regulation and labor market institutions matter in guiding employer options and choices around technology adoption, and the resultant outcomes for workers.

In industries with some presence of unions—health care, trucking, and grocery—our researchers identified examples of workers influencing the process of new technology adoption to create better outcomes for workers. However, even in these industries, our researchers found that broader societal and economic trends are likely to continue to push employers to use new technologies in ways that increase the challenges workers face on the job. In industries like non-food retail and warehouses, where unions are less common and where large firms are able to set the terms of competition, prospects for workers to experience beneficial effects from technological change are even bleaker.

Absent an intentional shift in our current approaches to technological change, the industries our researchers studied are likely to see employers use new technologies in ways that make job quality worse and widen economic and race and gender inequality in the labor market. So how do we change our course? We know that new technologies can be used in ways that support workers, but how do we get there? The findings of our studies suggest that achieving better outcomes for workers will take a multifaceted approach including industry-specific institutional and regulatory changes, broader policy changes, and workplace-based organizing.
Endnotes

1. There is of course a substantial and growing body of theoretical and empirical literature on technological change and work, including but not limited to the question of automation. For some recent examples see Acemoglu & Restrepo (2020); Agrawal et al. (2019); Hu (2022); Jarrahi et al. (2021); Kellogg et al. (2020); Moradi & Levy (2020); Rogers (2020). For a discussion of methodological approaches to studying technology and work, see Bailey & Barley (2020).


3. Carré et al. (2020).

4. Litwin (2020).


6. Benner et al. (2020); Carré et al. (2020); Gutelius & Theodore (2019).


11. For further discussion on automation and tasks, see: Acemoglu & Restrepo (2019); and Manyika et al. (2017).


15. For a deeper discussion of the ways employers can use algorithms in the workplace, see chapter 5 of Kresge (2020a).


17. Litwin (2020).


20. Benner et al. (2020); Carré et al. (2020).


22. Data collection on workers often serves another function besides monitoring, task direction and pace-setting: generating data to inform the development of new tools and machines to automate certain types of tasks.
Workers are also monitored as a by-product of employers’ use of video monitoring to track customers as well (e.g., for shoplifting or for tracking customer shopping habits). (Carré et al. 2020).  

Viscelli (2018), p. 7. Levy (2015) notes that certain regulations have increased in trucking: some Department of Transportation rules introduced over the past few decades have actually led to increased electronic monitoring of truckers.

Additionally, although labor is relatively inexpensive, the U.S. tax code favors employer investments in capital over investments in labor in a variety of ways, which may incentivize firms to pursue labor-replacing technologies in the long run (Acemoglu et al. 2020).

Connecticut and Minnesota passed similar bills, and one was proposed in Washington as well. Both chambers of the New York State Legislature have passed the Warehouse Worker Protection Act, though it has yet to be signed by the governor. (An Act Concerning Protection of
However, companies like Uber, Lyft, and Doordash continue attempting to weaken and overturn these laws. In 2020, Uber, Lyft and Doordash spent over $200 million in California to pass Proposition 22, which invalidated the law extending employment rights to many app-based workers. An Alameda County Superior Court Judge ruled the ballot measure unconstitutional in 2021, but it remains in effect during the app companies’ appeal. (Conger & Browning 2021; Lyons 2021).

Kresge (2020b). It’s important to point out that there are ongoing debates around the extent of unions’ legal right to bargain over employers’ decision-making regarding technology, versus the effects of their decisions regarding technology. See Ashford & Ayers (1987); Rasband (1989).

Platooning involves electronically linking a series of trucks. In human-human platooning, humans drive each truck, but the lead truck controls the speed and braking in the following truck(s). In human-drone platooning, the lead truck is driven by a human, and subsequent truck(s) are controlled by technology. (Viscelli, 2018).

Many other employers seriously neglected worker safety during COVID, for instance by supplying insufficient protective equipment or sick leave accommodations, or by not enforcing masking rules for customers.
References


The analyses, interpretations, conclusions, and views expressed in this report are those of the author and do not necessarily represent the UC Berkeley Institute for Research on Labor and Employment, the UC Berkeley Center for Labor Research and Education, the Regents of the University of California, or collaborating organizations or funders.
How Common is Employers’ Use of Workplace Management Technologies?
A Review of Prevalence Studies

Nina Mast and Lisa Kresge
## Contents

Introduction ..................................................................................................................................... 1

Limitations of the Current Research Literature ................................................................................. 2

Summary of Prevalence Study Findings ............................................................................................ 4

1. Government Studies.................................................................................................................. 4
2. Studies by Private Research and Consulting Firms ............................................................... 11
3. Studies by Technology Vendors ............................................................................................ 22
4. Trade Association Studies ........................................................................................................ 25
5. Other Tech Vendor Prevalence Indicators............................................................................... 26
Introduction

Over the last decade – and particularly since the onset of the COVID-19 global pandemic – the use of digital technologies in workplace management has received increased attention. Whether the focus is on the algorithmic management of delivery drivers, the productivity monitoring and evaluation of warehouse workers, or the apparent explosion in automated hiring software, it is clear that digital technologies have the potential to profoundly reshape the 21st century workplace.¹ However, we have only a weak understanding of how widespread these technologies are in US workplaces, why and how employers use them, and the range of impacts on workers.

The purpose of this working paper is to help fill this information gap. We provide an overview of existing research that attempts to measure the prevalence of employers’ use of workplace management technologies – i.e., technologies that are used to monitor, evaluate, or make predictions about workers, or assist or augment their tasks.

Specifically, we focus on firm-level adoption of the following technologies in the workplace: digitization of business information and cloud computing; hiring technology; human resources analytics; electronic monitoring; and emerging technologies like machine learning and artificial intelligence. Table 1 gives a fuller description of these technologies and common terms used to refer to them.

### Table 1: Technologies of Focus

<table>
<thead>
<tr>
<th>Tech type</th>
<th>Description</th>
<th>Additional Descriptors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitization and Cloud Computing</td>
<td>The process of converting analog information to digital form; prerequisites for investments in more advanced tech</td>
<td>“Software as a service (SAAS),” “platform as a service (PAAS)”</td>
</tr>
<tr>
<td>Hiring Tech</td>
<td>Includes the use of assessments and automated tools like applicant tracking systems (ATS) to make hiring decisions</td>
<td>“Talent assessment,” “predictive hiring”</td>
</tr>
<tr>
<td>HR Analytics</td>
<td>Collection and use of data about workers, both to evaluate workers and predict future performance</td>
<td>“Data analytics,” “people analytics”</td>
</tr>
<tr>
<td>Electronic Monitoring</td>
<td>The use of technological tools (software, sensors) to surveil or track workers</td>
<td>“Remote monitoring,” “performance tracking”</td>
</tr>
<tr>
<td>Emerging Tech</td>
<td>Includes investments in machine learning, computer vision, natural language processing, facial recognition</td>
<td>“AI,” “advanced technologies”</td>
</tr>
</tbody>
</table>

We collected studies for this paper based on an analysis of secondary literature and through monitoring industry, consultant, and HR field newsletters and publications.² Our geographic focus was the United States, although we included several important studies from the European Union. Despite differences between the EU and the US, these studies give an indication of the general state of technology adoption in western industrial economies, especially given the growing dominance of multinational corporations.

### Limitations of the Current Research Literature

While interest in digital workplace technologies is growing, there is a dearth of comprehensive, reliable data on the prevalence of firm-level adoption.³ Limitations of current research include:

- **No common measure of prevalence of firm-level adoption of workplace management technologies:** Organizations conducting surveys use a wide variety of metrics to measure prevalence, many of them indirect, making it difficult to distill overall trends. Examples of measures include firms’ investment or plans to invest in technology; technology adoption or planned adoption; and market share or value of a particular technology service. Most

---

² We conducted Google keyword searches for various technologies in Table 1 + “use” or “adoption” or “spending” or “investment” and limited our time frame to studies published within the past four years (with one exception for an old study that is widely-cited but has not been updated).

studies also include employers’ perceptions of and experiences with specific technologies, use cases, or goals for adopting certain technological tools.

- **Ambiguous or missing definitions of technologies:** The term “AI” is often undefined and used as an umbrella term that includes many disparate technologies. Also, consulting firms and vendors employ an array of similar-sounding terms such as “workforce analytics” or “people analytics” without providing clear definitions. As a result, it is difficult to ascertain exactly what these studies are measuring and how survey respondents are interpreting questions. Lack of definitional clarity also limits the ability to compare reports about similar technologies.

- **Methodological limitations and limited access:** Most consulting firms and vendors have proprietary datasets and only publish select results. In many cases they do not provide comprehensive explanations of their methods, including information about their respondents or how they recruited them. Because of these limitations, it is often impossible to assess the representativeness of their surveys or to evaluate potential sampling bias. Some reports, particularly market share reports by private research firms, provide only a very basic summary and charge for full access.

- **Unrepresentative samples in private survey data:** From what we are able to ascertain, firm surveys by vendors and private consulting firms are typically not nationally representative—in some cases, respondents are clients or contacts of the firm. Compared to representative government surveys, respondent firms in private surveys tend to be larger, publicly traded firms that typically adopt technology at higher rates than small firms. In the case of vendors, there are market incentives to demonstrate growing rates of adoption. However, often these private surveys can result in useful information, and so we include a number of them in this report.

- **Limited US government data collection on tech adoption:** The United States currently collects limited data about firm-level technology adoption in official government surveys. In an attempt to remedy this oversight, in 2018 the Census Bureau introduced a technology module in its Annual Business Survey (ABS). The technology module will be included for five years of the ABS, with new questions each year. The latest technology module includes some questions on worker effects from automating technologies, but very few questions related to workplace management technologies in particular.

---


5 See U.S. Census Bureau Center for Economic Studies 2018 and 2019 surveys below.
Summary of Prevalence Study Findings

Our goal is to understand the prevalence of employers’ use of workplace management technologies; however, very few studies directly measure the use of these technologies. Therefore, this section summarizes studies that in our assessment provide indirect indicators of workplace management technology adoption. We categorize the studies based on the entity that conducted and/or published the study: government studies, private research and consulting firms, vendors, and trade associations. For each study, we describe the characteristics of the sample and recruitment strategy, the prevalence measure used, our assessment of the study’s quality, and key findings. For most studies, we include all relevant information about the sample that was provided by the study authors. We attempt to evaluate the quality of the study according to metrics such as sample representativeness, respondent recruitment method, and sample size. Studies for which we could not evaluate the quality of the research, either because their methodology was vague or was not disclosed, are rated “Unknown.”

The paucity of research in this area makes it difficult to draw firm conclusions across studies. It does seem clear that firms’ adoption of workplace management technologies is still in its growth phase. None of the studies below find that the large majority of businesses are currently using this technology, and in general, firm-level adoption of advanced technologies remains low. Moreover, the tendency of consulting firms and vendors to survey large private firms (which typically adopt advanced technologies at higher rates) likely leads to an overstatement of adoption rates. That said, firms are increasingly digitizing their information systems and adopting cloud computing; these technologies are foundational to the adoption of more advanced technologies such as predictive analytics and artificial intelligence. The trendline, therefore, is very likely one of accelerating adoption.

1. Government Studies

Center for Economic Studies (2022)6

Study Overview: The Census Bureau’s 2019 Annual Business Survey (ABS) focuses on workforce impacts of artificial intelligence (AI), cloud services, specialized software, robotics, and specialized equipment. The survey was mailed to 300,000 nationally representative employer businesses in all private, non-farm sectors of the economy, and 208,000 responses were received, for a response rate of 69%. To gain a better understanding about the extent of workforce displacement due to emerging technologies, the 2019 ABS included questions about employer adoption of advanced technologies relevant for automation. The survey module defines artificial intelligence as “systems

with artificial intelligence perform functions including, but not limited to, speech recognition, machine vision, or machine learning” and describes each of these systems with examples of technology applications.7

**Prevalence Measure:** Adoption and workforce impacts of AI, cloud services, specialized software (business applications excluding AI), robotics, and specialized equipment (task-specific automation excluding robotics).

**Study Quality Assessment:** High

**Findings:**

- Tech adoption for AI (3%) and robotics (2%) is very low, and moderately more for dedicated equipment (20%), cloud computing (34%), and specialized software (40%).

- Although the share of firms adopting these technologies is relatively low, worker exposure is higher because the firms adopting these technologies are some of the largest companies in the US. For example, 13% of US workers are employed by firms that have adopted AI even though only 3% of firms have adopted these technologies. On the other end of the spectrum, 64% of US workers are employed by the 40% of firms using specialized software.

- Half (52%) of firms have not adopted any of these technologies, but firms that do adopt at least one technology are more likely to adopt multiple technologies.

- In terms of “exposure of US workers to automation,” the authors estimate that nearly 7% of workers are employed by firms adopting AI for automation purposes. However, worker exposure to automation is much greater for other technologies – 21% of workers work for firms using specialized software for automation purposes, 15% for cloud computing, 14% for dedicated equipment, and 10% for robotics. The authors suggest that “even though AI and robotics are more likely to be used to automate tasks, automation via dedicated equipment, specialized software, and cloud-based systems have been more important contributors on the aggregate due to their wider adoption and applicability.”

- The half of the respondents that did not adopt technologies reported factors that contributed to non-adoption. Of those 45-50% indicated that the technologies were not applicable to their business operation. Cost was the next most cited factor, with 7-9% reporting this as a limiting factor. AI, cloud, and specialized software are most adopted in the information, professional services, and finance, insurance, real estate industries, while robotics and specialized equipment are most adopted in manufacturing, healthcare, and agriculture.

For most firms that adopt technologies, their leading motivations are improving the quality or reliability of processes (68%-80% depending on technology) and upgrading outdated processes or methods (50%-64%), based on employment-weighted shares. Firms that adopt robotics (66%) and AI (54%) are motivated by automation, in terms of employment weighted shares.

Center for Economic Studies (2020)\(^8\)

**Study Overview:** The Census Bureau’s 2018 Annual Business Survey (ABS) provides comprehensive information on the diffusion of advanced technologies, including: artificial intelligence (AI), cloud computing, robotics, and the digitization of business information. The 2018 survey was the first time the ABS included questions related to technology adoption. The survey was sent to 850,000 firms in all private, non-farm sectors of the economy, and 583,000 responses were received. Importantly, the survey sample included many small and young establishments, which helps to provide an accurate representation of adoption patterns since these firms are “often underrepresented in private surveys of R&D and technology use,” according to study authors. Notably, the 2018 survey does not use the term artificial intelligence (AI) in the definition of advanced technologies often grouped under the umbrella of AI.\(^9\)

**Prevalence Measure:** Share of firms that store information digitally; firms’ expenditures on cloud computing services; firms’ adoption rates of advanced business technologies.

**Study Quality Assessment:** High

**Key Findings:**

- **Digitization:** Over 90% of firms that collect information on business functions (e.g., marketing or production) store at least one form of information digitally. Across all sectors, financial (84%) and personnel (72%) information are the most common sources of digitized information. Other areas of business function digitalization especially relevant to workers, such as customer feedback (53%) and production (46%), are less widely adopted. The manufacturing, information, and professional services industries have the highest rates of digitization, and adoption rates are correlated with firm size.

- **Cloud computing:** Firm adoption rates of cloud services is significantly lower than the rates of digitization, but is still fairly widespread. Firms are adopting cloud services across the full range

---


of business functions, such as all IT functions (46%), data storage (44%), customer relations (37%), and data analysis (31%). Large firms are the most likely to purchase cloud computing services. However, the authors note that “the relationship between cloud use and firm age is more nuanced” – among large firms, cloud use increases with age and then decreases, with the oldest firms reporting the lowest rates of adoption.

- Advanced business technologies: Adoption rates are low for advanced business technologies, which includes technologies that are often categorized as “AI,” such as “automated guided vehicles, machine learning, machine vision, natural language processing, and voice recognition software” as well as “radio frequency identification, touchscreens/kiosks for customer interface, automated storage and retrieval systems.” According to the authors, “across all AI-related technologies, the aggregate adoption rate for all firms in the economy is 6.6%.” In other words, “approximately 1 in 16 firms in the US are utilizing some form of AI in the workplace.” Importantly, rates of adoption among firms of each of the five technologies often considered AI – automated guided vehicles, machine learning, machine vision, natural language processing, and voice recognition software – range from less than 1% to slightly less than 3% individually.

- However, the share of workers exposed to these technologies is much higher because adoption rates tend to increase with firm size. In other words, even though few firms have implemented advanced technologies, these technologies impact a large portion of the workforce. Specifically, firms that have adopted at least one type of advanced business technology employ more than 40% of all workers, and firms that have digitized at least one form of information and have invested in cloud services – the building blocks of more advanced technologies – employ more than 90% of all workers.

European Commission’s Digital Economy and Society Index (DESI) Integration of Digital Technology (2022)¹⁰

Study Overview: The annual Digital Economy and Society Index (DESI) summarizes indicators on Europe’s digital performance and tracks the progress of EU countries. The DESI 2022 reports are based mainly on 2021 data and present the state of the digital economy and society in the first year of the pandemic. The index measures EU member states’ progress on four broad dimensions: human capital, connectivity, integration of digital technology, and digital public services. The findings reported here are from the Integration of Digital Technology dimension only. Data sources

include data collected and verified by the national statistical offices or by Eurostat, data collected by Ipsos and iCite, and survey results reviewed by the Digital Single Market Strategic Group.\textsuperscript{11}

**Prevalence Measure:** Intensity of digital tech use by firms; use of big data analysis; investment in cloud computing; AI adoption.

**Study Quality Assessment:** High

**Findings:**

- Just over a third (34\%) of large enterprises analyze big data internally from any data source or externally, while only 14\% of small and medium enterprises (SMEs) analyze big data. The industries most likely to analyze big data are travel agencies/tour companies (28\%) and the publishing industry (28\%); the manufacturing industry (10\%) was the least likely to analyze big data.

- One-third (34\%) of EU companies have invested in cloud computing technologies. Large enterprises have incorporated cloud computing (60\%) at a much higher rate than SMEs (33\%). Cloud computing adoption is highest in the internet and communication technology (ICT) industry (66\%) and the lowest in the construction industry (26\%).

- Only 8\% of companies report adopting AI technologies. However, large enterprises are much more likely to report use of AI technologies (29\%) than SMEs (7\%). Not surprisingly, the ICT industry is at the forefront of AI adoption (25\%), whereas the construction and transportation/storage industries are less likely to adopt AI technologies (both at 5\%).

**European Commission (2020)\textsuperscript{12}**

**Study Overview:** In early 2020, the European Commission fielded the first EU-wide survey on artificial intelligence adoption at 9,640 enterprises of all sizes (the gross sample was about 20 times this size) across the EU27, Norway, Iceland, and the UK. The survey was administered through computer-assisted telephone interviewing (CATI), which helped to coordinate national interviewers and to obtain representative country estimates. The overall response rate was 7\%. Respondents included any “employee who is familiar with how technology is used within the firm.”

**Prevalence Measure:** AI awareness; AI adoption; AI sourcing; external and internal obstacles to AI.\textsuperscript{13}


13 We only include findings on AI adoption and sourcing; see the full report for more detail.
Study Quality Assessment: High

Findings:

- Overall, 42% of respondents use at least one AI technology in their business operations; among those respondents, 17% use one technology and 25% of respondents use two or more AI technologies. On the other hand, 40% of respondents are not using and not planning to use AI, and 18% of respondents are not currently using but plan to adopt AI in the next two years.

- There is a positive relationship between the number of AI technologies an enterprise currently uses and its plans to increase usage in the future. For instance, 52% of firms that use one form of AI technology plan to use AI more in the future, and only 6% plan to use it less. At firms that use four AI technologies or more, 68% plan to use AI more in the future and only 2% plan to use it less.

- The most common use cases for AI technologies across the EU27 are: process or equipment optimization (11% use, 13% plan to use); anomaly detection (13% use, 7% plan to use); process automation (12% use, 11% plan to use). Sentiment analysis is the least adopted technology (3% use, 3% plan to use).

- Large enterprises are most likely to adopt AI. Over half (55%) of companies with 250 employees or more use at least one AI technology; at the other end of the spectrum, only 39% of companies with between five and nine employees use at least one AI technology.

- By industry, information and communication technologies (63%); education (49%); human health; social work; and manufacturing (all 47%) have the highest rates of AI adoption. AI adoption is lowest among waste management (31%), construction, transport, and food (all 36%) sectors.

- Businesses typically acquire their AI technologies from external sources. A majority (59%) of enterprises purchase ready-to-use systems (systems not requiring customization) from external sources, while 38% of companies hire external providers to develop customized tools. Only between 20% and 24% of firms choose to develop AI solutions in-house, either by modifying commercial systems or open-source systems.
Study Overview: The European Foundation for the Improvement of Living and Working Conditions (Eurofound), in collaboration with Cedefop, compiled and analyzed data from the 2019 European Company Survey (ECS), which includes responses from 21,869 establishments with 10 or more employees in sectors engaged in “market activities” across the 27 European Union Member States and the United Kingdom. Researchers contacted establishments via telephone and attempted to “identify a management respondent and, where possible, an employee representative respondent” to fill out the online questionnaire. The 2019 ECS included questions about employers’ “use of data analytics for employee monitoring.” The survey authors defined data analytics as “the use of digital tools for analyzing the data collected within the establishment or from other sources.” This report also incorporates data from a 2019 semi-structured questionnaire conducted by the Network of Eurofound Correspondents and secondary research.

Prevalence Measure: Employer use of data analytics to improve production processes, monitor employee performance, or both.

Study Quality Assessment: High

Findings:

- Half (51%) of EU27 establishments report using data analytics in their business operations. Among the respondents using data analytics, 24% report using data analytics solely for process improvement, 5% report using data analytics solely for monitoring of employee performance, and 22% report use for both purposes.

- Employee monitoring is most prevalent in the transportation industry (36%). Other industries with relatively high levels of employee monitoring are manufacturing (industry) (~28%), and wholesale, retail, and accommodations (~27%), other services (~26%), financial services (~24%), and construction (20%).

- Larger firms are more likely to monitor employees – 40% of large establishments (250 or more employees) report using data analytics to monitor employees, while only 25% of small establishments (10 to 49 employees) report using data analytics for this purpose.


15 Some percentages are approximate based on data reported figure 2 in the report; exact percentages were not included in the report.
● Firms with a recognized employee association or employee representation were more likely to report monitoring employee performance (34%) than firms with no employee representation (24%).

2. Studies by Private Research and Consulting Firms

➢ Deloitte Human Capital Trends (2020)\textsuperscript{16}

\textbf{Study Overview:} Deloitte’s 2020 Human Capital Trends report is based on a survey of 9,000 HR and business leaders in 119 countries. One-quarter (26%) of respondents are from Western Europe, 19% are from Latin and South America, 14% from North America, 14% are from Central and Eastern Europe, 9% are from Asia, 9% are from Africa, and the remaining 11% are from Nordic Countries, Middle East and Oceania. Respondents also work in a variety of industries including consumer products (19%), professional services (17%), technology, media, and telecom (14%), financial services (13%), among others. Half (51%) of the respondents work for companies with fewer than 1,000 employees, 27% work for companies with 1,001 to 10,000 employees, and 22% work for companies with more than 10,001 employees.

\textbf{Prevalence Measure:} Production of workforce data; employer perception of AI; investments in AI.

\textbf{Study Quality Assessment:} Useful, but not representative

\textbf{Findings:}

● Organizations’ interest in workforce data is increasing, with more than half (53%) of respondents reporting increased interest among leadership in the past 18 months. A very large majority (83%) of respondents report that “their organization produces information on the state of their workforce,” but only 11% of organizations “produce the information in real time” and 43% either produce it irregularly or don’t produce it at all.

● Among organizations that have adopted AI within their organization (76%), the primary reasons cited are to assist workers (60%), to replace workers (12%), or to oversee workers (4%). Nearly one-quarter (24%) of participating organizations do not use AI in their operations.

● Among organizations that use “AI primarily to assist workers,” more than half are using AI “to improve consistency and quality” (58%), and about a quarter more are using AI to “improve productivity” (26%). Only 16% of participating organizations are “using AI

primarily to assist workers in developing insights.” And only 17% of respondents say that their organizations are investing heavily in training employees to support AI adoption.

- A large majority (85%) of respondents reported that “the future of work raises ethical challenges,” but only one-quarter (27%) of respondents report having “clear policies and leaders in place” to address these challenges. The top reasons for the focus on ethical concerns cited by respondents include “legal and regulatory requirements” (38%), “rapid adoption of AI in the workplace” (34%), “changes in workforce composition (e.g., growth of the alternative workforce)” (32%), and “pressure from external stakeholders (e.g., investors, customers, special interest groups, etc.)” (29%).

- Moreover, many respondents indicated that their organizations were “not ready” to address issues related to the future of work. For example, respondents who rated concerns such as “use of algorithms to influence decision-making” and “use of AI and data to monitor individuals in the workplace,” 37% and 31% respectively indicated they were not ready to address these concerns.17

**Deloitte State of AI (2021)**18

**Study Overview:** Deloitte’s 2021 State of AI report is based on a survey of 2,875 business and IT executives from 11 countries and 6 industries who have involvement in AI development, investment, or strategic deployment within their organizations. To supplement the survey, Deloitte also conducted 17 interviews with AI experts in multiple industries.

**Prevalence Measure:** Employer perception of AI; investments in AI.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- Participating companies report using an average of 3.5 AI applications in their business operations.

- Two-thirds (66%) of respondents view AI as important to “remaining competitive”s, but only 40% agree that their company has an “enterprise-wide AI strategy” in place, and 40% agree that their leadership has communicated “a vision for AI that will significantly change” operations.

---

17 For this question, respondents selected their top 3 ethical concerns and then rated their “readiness” to address the concern.

Thirty-seven percent of survey respondents report significant investment in “change management, incentives, or training activities to help people integrate new technology into their work.”

One-quarter (26%) of respondents say “employees trust AI-derived insights more than their own intuition,” and 19% of respondents report that employees are concerned about AI initiatives. Firms identified in the report as “high-achieving organizations” are more than twice as likely to report fear about AI integration than “low-achieving organizations.” According to the study authors, “fear may be a positive indicator that an organization’s AI vision is bold.” However, report authors point out that “high-achievers” report “little desire to reduce employee headcount as well as high investment in training and change management.”

Most (74%) respondents report having “two or more ecosystem relationships” with technology vendors.

**Digital.com and Pollfish (2021)**

**Study Overview:** Digital.com commissioned Pollfish to conduct an online survey of American employers’ use of remote work monitoring software, what they’re looking for, and what the results have shown. The survey was conducted in September 2021 and included a sample of 1250 employers with all or some of their employees working remotely.

**Prevalence Measure:** Rate of employer use of electronic monitoring; goals and results of monitoring.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- Among companies with employees who work remotely, 60% are “using monitoring software to track employee activity and productivity,” and another 17% are considering it.
- The top reason employers adopt monitoring software is to “understand how employees are spending their time” (79%). Employers also want to know whether employees are “working a full day” (65%), and make sure they are not “using work equipment for personal use” (50%).
- The most common types of software used by responding employers are web browsing and application use trackers (76%), random screenshot capture systems (60%), application and content blockers (54%), and keystroke logging systems (44%).

---

• Among companies using monitoring software, 86% have informed their employees and 14% have not.

• Eighty-eight percent of employers report firing workers after implementing a monitoring system.
  ○ One-quarter (25%) of employers terminated between 1 and 10 workers based on information gathered in productivity monitoring.
  ○ Twenty-one percent fired between 51 and 100 employees.

• Advertising and marketing (83%), computer and information technology (77%), and construction (71%) are the top three industries that have adopted monitoring software, among companies surveyed.

IBM Institute for Business Value (2017)²⁰

Study Overview: The IBM Institute for Business Value (IBV) and Oxford Economics surveyed 550 corporate executives with a focus on organizational operations about digital systems in use by their organizations, including AI/machine learning and intelligent automation. Respondents included executives from organizations with at least $500 million in revenue in thirteen industries (with 6-9% of respondents from each industry) and a dozen countries around the world.

Prevalence Measure: Adoption of predictive analytics; machine learning/AI; adoption of the building blocks for AI (cloud, mobile, Internet of Things (IoT) technologies).

Study Quality Assessment: Useful, but not representative

Findings:

• One-quarter (25%) of respondents are currently using predictive analytics in their organizations, but 23% are piloting and 30% are planning to adopt this technology. The report defines “predictive analytics” as “the practice of predicting outcomes using statistical algorithms and machine learning.”

• Sixteen percent (16%) of respondents are using machine learning/AI in their organizations, but 20% are piloting and 42% are planning to adopt these technologies. The report defines “artificial intelligence/machine learning” as “the application of systems equipped with software that simulates human intelligence processes, including learning without explicit instructions.”

● Of respondents citing “some positive impact” and “substantial positive impact” from “robots and other intelligent machines,” the top three benefits include increasing efficiency (48%), increasing productivity (46%), and extending human capabilities (43%); lower on the list (8th) is working autonomously without human intervention (38%).

● Close to half of responding organizations are implementing Cloud, mobile, and IoT technologies – important precursors to machine learning – in some parts of their business.
  ○ Nearly three-quarters (74%) of respondents report their organizations are currently using cloud in some (58%) or all (16%) parts of the business, and 42% anticipate using cloud applications in all parts of their businesses in the next three years, including the 16% already doing so.
  ○ Similarly, 68% of respondents report mobile technologies are in use in some (52%) or all (16%) parts of the business, and 41% plan to use mobile devices throughout operations in the next three years, including the 16% who are already using mobile devices.
  ○ IoT is less widely adopted, with 55% of respondents indicating IoT use in some (48%) or all (7%) parts of their business. However, 61% plan to implement or continue to use IoT in some capacity, and 22% plan to implement or continue to use IoT across the firm in the next three years.

● Regarding broader organizational changes to accommodate advanced technologies, 60% of businesses are “optimizing business processes for automation,” 47% are “training humans to work with machines,” 31% are “incorporating machines that adapt and learn to make recommendations,” 27% are “changing employee behaviors toward machines,” and 18% are “increasing use of natural language processing.”

● Telecommunications, healthcare, retail, automotive, and banking and financial services, are at the forefront of “intelligent automation” adoption, based on average use of emerging technologies – artificial intelligence/machine learning, natural language processing, robotics, and predictive analytics – within the industry.

➤ McKinsey (2021)21

Study Overview: McKinsey Global conducted their 2001 online McKinsey Global Survey on AI between May and June 2021. In total, 1,843 organizations participated in the survey, “representing the full range of regions, industries, company sizes, functional specialties, and tenures.” Only Respondents who indicated that their organizations had “adopted AI in at least one function” of AI (n=1,013) and were asked additional questions about AI use. The report authors weighted

responses to “adjust for differences in response rates” and reflect “the contribution of each respondent’s nation to global GDP.”

**Prevalence Measure:** Rate of AI adoption; AI use cases; adoption rate of strategies to mitigate AI bias.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- Over half (56%) of all respondents report using AI (e.g., machine learning, computer vision, or natural language processing) in at least one function in their operations.
- The top three AI use cases among firms adopting AI, are “service-operations optimization” (27%), “AI-based enhancement of products” (22%), and “contact-center automation” (22%). Other AI use cases that could potentially impact workers include “customer service analytics” (17%), using AI to optimize “talent management” (8%), or for “performance management” (8%).
- The report presents survey findings on 25 core and advanced best practices related to AI. Fewer than half of respondents are implementing best practices related to informing, consulting, and training users on their AI models.
- Firms are particularly concerned about AI risks in the areas of cybersecurity, regulatory compliance, and explaining how AI models make decisions. Respondents are comparatively less concerned with mitigating AI risks related to equity and fairness and workforce/labor displacement, among others. Fewer than half of organizations engage in risk-mitigation practices such as training and testing data and measuring model bias and accuracy.

---

**PwC AI Business Survey (2022)**

**Study Overview:** PwC Research surveyed 1,000 “US business and technology executives involved in deploying AI strategies” in their respective organizations between January and February 2022. Half of the respondents have C-suite titles. Nearly one-quarter (23%) of the respondents work for companies with revenues of $5 billion and up. Industries represented in the sample include:

---

22 See Exhibit 6 of the 2021 McKinsey & Company report for the full list of risks that firms identify as relevant and are working to mitigate.

23 The report authors do not report total percentages for all respondents who have adopted AI and instead separate responses among “high performers” (defined as organizations that report at least 20% of their earnings before interest and taxes (EBIT) as attributable to AI) and “all other respondents.” Given that the authors do not provide the total number of respondents in each category, we cannot calculate total responses for these questions.

24 Anand Rao and Brett Greenstein, “PwC 2022 AI Business Survey,” PwC Research, 2022,
industrial products (34%), retail and consumer (19%), financial services (17%), tech, media and telecommunications (15%), health industries (10%), and energy, utilities and mining (5%).

**Prevalence Measure:** AI adoption; use cases and goals for AI; responsible AI plans.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- One-quarter (26%) of all respondents report “processes fully enabled/widespread adoption” of AI technologies into their operations and 29% of all respondents report that they have implemented limited AI use cases.

- Eighteen percent of all respondents have “promising proofs of concepts and are looking to scale” AI technologies into their operations; 18% have tested “proofs of concepts with limited success;” and 9% are “not yet using, but considering” integrating AI into their operations.

- The top 3 business objectives for AI initiatives cited by respondents include increasing productivity through automation (29%), improving customer experience (28%), and improving decision-making (27%). Slightly lower on the list of objectives are improving employee experience and skills acquisition (24%), and improving retention and recruitment (18%).

- Just over one-third (36%) of all respondents report plans to use AI simulations, such as “digital twins,” to hire and train employees in 2022.

- Fewer than half of respondents report plans to take steps in 2022 “to develop and deploy AI systems that are responsible, that is trustworthy, fair, bias-reduced and stable.”

---

25 Percentages of “all respondents” listed here were calculated by the authors of this report. The PwC report does not present percentages for all respondents for each question, and instead the authors present the information separately for “AI leaders” (respondents who met a criteria for taking a “holistic approach to AI”) and “others” (the remaining survey participants). We calculated the percentages listed here by applying the reported percentages for each group to their respective number of participants and then dividing the combined total by the full sample size.

26 The PwC 2022 AI Business Survey asked about a wide range of best practices related to responsible AI. For example, 46% of all respondents reported that they planned to “confirm that AI is compliant with applicable regulations” in 2022; this was the most common practice cited by respondents, other practices, such as “review to be sure third-party AI services meet standards” were cited less often (32%). See the chart titled “Responsible AI actions planned for 2022” for more detailed information.
PwC HR Tech Survey (2022)\(^\text{27}\)

**Study Overview:** PwC administered their 2022 PwC Human Resources Technology survey to 688 HR leaders based in the United States about their HR technology goals, experiences, and challenges.

**Prevalence Measure:** Adoption of HR tech; use of employee monitoring and productivity tracking software.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- Nearly all participating companies monitor or plan to monitor their remote workforce – 37% have already implemented a productivity tracking system that generates performance metrics for remote workers, 35% are considering or developing a plan, 22% have a plan for introducing a productivity tracking system but have not yet implemented it, 3% do not plan to monitor remote workers, and 3% are unsure.

- With respect to cloud HR tech vendors, 44% of companies report they are “unlikely to switch vendors at the end of their subscription term,” 36% say it is likely they will switch, and 19% are unsure. Budget issues (28%) and problems with integration with other technology vendors (27%) are the most common challenges reported by survey participants.

- Respondents cite implementation costs (23%), the lack of a compelling use case for the technologies (20%), and cybersecurity concerns (19%) as the top reasons preventing them from using disruptive technologies, such as robotic process automation (RPA), Internet of Things (IoT), artificial intelligence (AI), blockchain, and virtual reality (VR). Data privacy concerns (16%) is another reason preventing adoption of these technologies among respondents.

PwC HR Tech Survey (2020)\(^\text{28}\)

**Study Overview:** PwC Research conducted a survey of 600 HR and IT leaders from six continents in September 2019. Most (61%) of the respondents have C-suite and VP titles, and 48% of firms represented in the sample report annual revenues of over $1 billion. Survey participants work for employers from a variety of industries including health services, manufacturing, retail, and technology.


Prevalence Measure: Spending on HR tech; goals and use cases for HR tech; perceptions about effectiveness of HR tech.

Study Quality Assessment: Useful, but not representative

Findings:

● Three-quarters (74%) of companies surveyed plan to increase spending on HR tech in 2020. Survey respondents are particularly focused on talent acquisition tools (49%), employee experience portals (48%), and skills mapping/career path systems (46%).

● Half (50%) of respondents report using multiple vendors and 39% plan to contract with additional vendors over the next three years.

● Study authors found a gap between C-suite executives’ perceptions of the effectiveness of HR technologies and those of the managers who use the technologies. For example, half (50%) of C-suite executives think HR tech has been “very effective” at increasing productivity/efficiency, but only 22% of managers agree.

● In order to increase HR tech adoption among employees, participating companies use training (50%), leadership communication (43%), incentives (30%) and gamification (20%).

● Core HR systems, such as benefits administration (51%) or payroll tools (48%), provide companies more value than talent management (37%) and workforce analytics (38%) systems, according to respondents.

● While two-thirds of survey participants report that they are able to produce “dashboards to optimize staffing based on analysis of hours, absenteeism, and overtime data,” only 39% say they are able to produce dashboards that can give insight “on which employees are critical for future success based on past performance, skills and competencies.”

RedThread (2020)²⁹

Study Overview: In 2020, RedThread surveyed 47 people analytics technologies (PAT) vendors, 60% of which are small firms with fewer than 100 employees. A PAT vendor is defined as “a company offering software that enables people analytics, designed intentionally to use data about people.” Vendors completed a 317-question survey covering topics such as system capabilities, user capabilities, and areas of focus for analytics. RedThread also polled 132 employers who are customers of the vendors to identify how they use people analytics and the strengths and weaknesses of the vendors they use. Of the customer respondents, about a third work in a people

analytics function. To be included in the study, each vendor was required to have at least five
customer reviews.

**Prevalence Measure:** Growth rate and market value of people analytics technologies; use cases for
PAT across vendors.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- RedThread identified 121 people analytics technologies (PAT) on the market today. The
  market overall is growing quickly, with a 35% growth rate between 2019 and 2020, a 55%
  compound annual growth rate (CAGR) for the last four years, and an estimated overall
  market value of $1.5 billion for 2019.

- Primary areas of focus for PAT vendors are: employee engagement (67%); employee
  experience (58%); diversity and inclusion analysis & monitoring – including pay equity
  analysis (52%); performance management (48%); and learning and development (42%).

- In terms of system capabilities and data sources, 40% of vendors use machine learning/deep
  learning to analyze unstructured data from voice (audio), image, and video data sources;
  one-third (33%) of vendors are analyzing “digital exhaust” captured from employee
  activities, such as email, computer file transfers, computer logs, etc.; one in four (40%)
  of vendors conduct sentiment analysis of employee communications, but only 26% use
  advanced natural language processing (NLP) for this analysis.

- Fewer than a third of vendors (28%) allow employees to see all the information collected on
  them, 23% let employees correct data about them, 15% allow employees to see insights
  based on passive data, and only 8% alert employees to the types of analyses being run on
  them.

- Some vendor systems: enable employees to share insights with others (28%), allow
  individual employees to compare their data with organizational level data (27%), or
  recommend actions to take (26%).

- On average vendors reported integrating data from eight different types of vendors. Most
  commonly the reported integrations with with core HR (HRIS) systems (89%); other
  integrations include: cloud-based technologies (60%), employee/candidate survey (60%),
  sales/CRM (57%), learning technologies (55%), work technologies (55%), and talent
  management (51%), among others.

- Around two-thirds of single solution vendors report developing design guidelines and
  policies around data collection (71%), sharing insights (68%), and data access (66%); however,
  multisource analytics platforms that often do not have direct interaction with
  employees are less likely to have these policies in place.
Sierra-Cedar (2019)30

Study Overview: The 2019 Sierra-Cedar HR Systems Survey sampled respondents from 1,892 organizations from around the world employing a total of 22.2 million employees and contingent workers in aggregate. Respondents were recruited using the following outreach methods: associations, vendors and media outlets; podcasts and webinars; radio shows; social outreach; clients; prior respondents; and prospects and contacts. Businesses with fewer than 2,500 employees make up 61% of respondents, while businesses with more than 10,000 employees make up 19% of respondents. Top industries are: manufacturing (15%), healthcare (13%), and financial services (11%).

Prevalence Measure: Uses of analytics and emerging technologies; methods of data capture and implementation challenges.

Study Quality Assessment: Useful, but not representative

Findings:

- Only 12% of participating organizations have a strategy for aggregating their “employee data footprint,” whereas 12% of respondents say they have a strategy in development and 76% report having no strategy.
- Respondents report multiple strategies for capturing employee data “beyond HR systems.” Exit interviews (86%) and employee surveys (72%) are the most popular common methods for capturing employee data, but wearables/badges/RFID (61%), and video monitoring (53%), pulse surveys (44%), internet/screen monitor (37%), social media (25%), mobile devices (25%), biometric sensors (23%), audio monitoring (16%), and environmental sensors (12%) are not far behind.
- Among the top uses for HR analytics among survey respondents are “cost management” (52%), “compliance risk management” (49%), “improved engagement” (47%), “improved retention” (47%), and “acquiring top talent” (39%).
- Seventeen percent (17%) of all respondents are currently using HR tech for predictive analytics for HR, while another 36% are considering it. Among emerging tech firms, 50% are using HR tech for predictive analytics, with another 44% considering it.

31 Sierra-Cedar, slides 13 and 29
3. Studies by Technology Vendors

- Bloomberg Tax & Accounting (2019)\textsuperscript{32}

**Study Overview:** Bloomberg’s Tax & Accounting team conducted a Payroll Benchmarks Survey in late 2018 among a sample of payroll professionals drawn from their national database of payroll professionals and executives. A total of 158 payroll professionals participated in the survey, representing non-manufacturers (54%); manufacturing (22%); and nonbusiness organizations, such as government entities, membership organizations and associations, health care facilities, educational institutions, and social services organizations (25%). Most participating organizations employed at least 1,000 workers (63%), whereas 34% had fewer than 1,000 employees, and 3% of respondents did not report their number of employees.

**Prevalence Measure:** Use and sourcing of payroll systems; adoption of automated time and attendance functions.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- Most respondents (73%) report using an employee self-service system for payroll operations; 62% use a web portal for payroll; and 41% have adopted cloud computing for some payroll data storage operations.

- Over two-thirds (69%) of respondents say they outsource some payroll functions to other organizations (vendors), while 31% do not outsource payroll operations. Of those that outsource payroll, only 4% report their payroll is completely outsourced to vendors.

- A large majority (79%) of respondents answering questions related to timekeeping practices report using some automated time and attendance functions, and 61% report receiving time-worked data electronically, and 27% of respondents say that at least three-quarters of their time-worked data was submitted electronically.

- Nearly all (99%) participating organizations pay employees with direct deposit; however, 74% report issuing some paper paychecks, 29% pay some employees with payroll cards, and 2% have introduced mobile payment options for employees.

---

ExpressVPN and Pollfish (2021)³³

Study Overview: ExpressVPN collaborated with Pollfish to survey 2,000 employers and 2,000 employees “who work in a remote or hybrid capacity” to gauge the extent to which employers monitored employees, the effects of monitoring, and the likelihood monitoring might continue to increase in the future. Pollfish recruits respondents through “random device engagement,” in which potential respondents are recruited via mobile apps they are already using.

Prevalence Measure: Employer adoption of remote worker monitoring software.

Study Quality Assessment: Useful, but not representative

Key Findings:

- More than three-quarters (78%) of employers report using software to monitor and track employee performance and/or internet activity, and yet 83% of employers report having ethical concerns about employee monitoring.

- Most participating employers report regularly recording and storing data from various communication channels: email (94%), calls (87%), video (87%), messages (85%).

- The most common surveillance activities reported by participating employers are: websites visited/time spent on various websites (66%), apps used/time spent on apps (53%), and real-time screen monitoring (53%).

- Slightly more than half (53%) of employees report knowing their employers monitor their activities. Study authors report that “1 in 3 employees don’t believe their employers are actively monitoring their online activities, and 15% didn’t even know that was possible.”

- The majority (59%) of employees report feeling stress and anxiety about their employer’s monitoring activities, with 41% “constantly wondering whether they are being watched.” Employees also report feeling pressure to “be actively online” (38%), “work longer hours” (36%), “work more and/or an equal amount of time as my colleagues” (36), or “take fewer breaks” (32%) because of employer monitoring.³⁴

- Forty-six percent of employers say they have used findings from remote worker monitoring to fire employees.

- The study authors indicate that 73% of employers report having “used stored email, calls, messages, or videos to inform their decisions on performance reviews and 46% report having used this information “to monitor the potential formation of workers’ unions.”


³⁴ The report includes two different percentages for employee stress 56% and 59%.
Study Overview: As a part of its ATS Tip feature, JobScan (an online resource for job applicants) collects crowdsourced data about companies’ use of applicant tracking systems, verifies that information, and then uses it to provide ATS-specific tips to applicants. To analyze Fortune 500 companies’ use of ATS systems, JobScan compiled and cross-checked the crowdsourced data, and filled in gaps by manually researching Fortune 500 applications for which they did not have any information.

Prevalence Measure: Use of applicant tracking systems by Fortune 500 employers.

Study Quality Assessment: Useful, but methods not reported

Findings:

- All but six Fortune 500 companies (99%) use an applicant tracking system (ATS). JobScan was able to identify the specific ATS vendor for 482 of the Fortune 500 companies.

- The six companies that do not appear to use an ATS are mainly holding or parent companies, such as Berkshire Hathaway. However, some of Berkshire Hathaway’s subsidiary businesses do use an ATS. For example, GEICO and United Airlines both use Taleo and Dairy Queen uses SilkRoad.

- The ATS vendors most often used by Fortune 500 companies are Workday, Taleo, SAP SuccessFactors, IBM Kenexa BrassRing, iCIMS, and ADP. Workday has the largest market share (26%) of Fortune 500 firms.

- Many companies use multiple ATS for different divisions. For example, Walmart uses Workday, BrassRing, and Greenhouse.

Study Overview: In October 2021, in collaboration with hotel management platform Stayntouch, NYU graduate students conducted a 21-question survey of 525 respondents who own, manage, or work at hotels in order to give the hospitality industry a better understanding of technology use trends and their effect on hotel operations and the guest experience. Researchers also conducted five interviews with hoteliers and four interviews with vendors. The respondent sample included hotel operators from independent and branded hotels that serve primarily business and/or leisure


Most respondents hold executive job roles, such as owners (30%), general managers (20%), other management executive roles (15%), or work in finance, revenue, sales, or marketing (17%).

**Prevalence Measure:** Use of and pandemic-related increase in use of technological tools at hotels, including: “contactless” experience tools like self-check-in and digital payment; process optimization tools like automated housekeeping task management; and chatbots.

**Study Quality Assessment:** Useful, but not representative

**Findings:**

- Almost half (49%) of respondents implemented automation tools, such as housekeeping task management systems, prior to the pandemic; 12% implemented automation tools during the pandemic; and 11% plan to implement automation in 2022.

- Self-service check-in increased substantially with the pandemic with 25% of respondents adopting these systems; 38% of respondents offered self-service check-in prior to the pandemic, and 12% plan to implement these systems in 2022.

- The use of chatbots increased 32% during the pandemic. Only 15% used chatbots prior to the pandemic, but an additional 5% implemented them during the pandemic, and 10% plan to implement them in 2022 (a 53% increase in usage compared to prior to the pandemic).

### 4. Trade Association Studies

➢ **ePolicy Institute and American Management Association (2007)**

**Study Overview:** The 2007 Electronic Monitoring & Surveillance Survey was co-sponsored by American Management Association (AMA) and the ePolicy Institute. There were a total of 304 respondents from six major industries in the United States. Survey respondents represent a wide range of company sizes, with 12% of respondents employing 5,001 or more workers, 10% employing 2,501-5,000, 12% employing 1,001-2,500, 12% employing 501-1,000, 27% employing 101-500, and 27% employing 1-100.

**Prevalence Measure:** Employer engagement in various types of employee monitoring and use of disciplinary action in response to policy violations.

**Study Quality Assessment:** Useful, but not representative

---

Findings:

- Internet: of the 66% of companies that monitor Internet connections, “65% use software to block connections to inappropriate websites.”

- Email: 43% of responding companies monitor email, 96% track incoming and outgoing messages (external email), and 58% monitor messages sent among employees (internal email). In terms of monitoring methods, “73% of organizations use technology tools to automatically monitor e-mail, and 40% of employers assign an individual to manually read and review e-mail.”

- Phone: 45% of companies monitor time spent on the phone and the numbers called, an increase of 9% between 2001 and 2007. Additionally, 9% monitor employees' voicemail messages, and 16% of companies record phone conversations, up 9% from six years earlier (2001). Most employers report that they notify employees of monitoring phone use (84%) and voicemail (73%).

- Computer: 45% of employers track content, keystrokes, and time spent at the keyboard, one-third (32%) do so on an ongoing basis; 43% store and review computer files.

- Video: nearly half (48%) of the companies reported using video cameras to monitor for theft, violence, and sabotage, up 33% between 2001 and 2007. Use of video surveillance to track employees’ job performance is not common among participating companies, with only 7% reporting this practice.

- Movement: few companies use Assisted Global Positioning or Global Positioning Systems (GPS) satellite technology; respondents report using GPS to track company vehicles (8%), monitor cell phones (3%), and monitor employee ID/Smartcards (fewer than 1%).

5. Other Tech Vendor Prevalence Indicators

HR Tech Radar (2021)\(^{38}\)

Source Overview: HRTechRadar provides consulting services to connect start-ups with investors. To compile this report, HRTechRadar founder, Anita Lettink, tracked “investment news from sources across the world in several languages” to identify public VC deals for HR technology vendors.

Prevalence Measure: HR Technology funding activity; HR industry unicorns (privately start-ups with a value of over $1billion); funding by HR Tech service function

Study Study Quality Assessment: Useful, but not representative

\(^{38}\) Lettink, Anita. 2022. “With $12B in Funding, 2021 Was HR Tech’s Best Year Ever!” HRTechRadar, January 10, 2022. [https://hrtechradar.com/hr-tech/with-12b-in-funding-2021-was-hr-techs-best-year-ever/](https://hrtechradar.com/hr-tech/with-12b-in-funding-2021-was-hr-techs-best-year-ever/)
Findings:

- In 2021, Venture Capital firms invested over $12 billion dollars in HR technology companies in 330 funding deals; this is more than the combined total for the two years leading up to 2021.
- Twenty-one HR technology vendors were valued at more than $1 billion (unicorns).
- Most HR technology companies are headquartered in the US, but many company founders move operations to the US or UK prior to seeking funding.
- Human Capital Management (HCM) and payroll services (e.g., core HR systems including time management, scheduling, payroll) received the most funding ($4.6 billion), talent management (e.g., retention, engagement, development) received $1.9 billion, and talent acquisition (e.g., recruiting and hiring) received $1.5 billion.

The Business of Business (2021)\(^{39}\)

Source Overview: The Business of Business (B2, formerly Thinknum Media) is a tech-oriented business publication. In February 2021, B2 published an article on the increased employer interest in monitoring remote workers amid the COVID-19 pandemic. The article reports average daily pageviews of four electronic monitoring software vendors over a five-year period (January 2016 to 2021) based on data from their proprietary web-scraping tool, Thinknum Alternative Data. The vendors – Workpuls, Time Doctor, ActivTrak, and Teramind – all have similar features, including activity tracking, screen recording, and the ability to track activity without the employee’s knowledge. In addition to these main features, Teramind also has a keylogging function, which records workers’ keystrokes.

Prevalence Measure: Average daily pageviews of electronic monitoring vendor websites.

Study Study Quality Assessment: Useful, but not representative

Findings:

- For all four vendors, average daily pageviews peaked in July 2020 and have declined considerably since then but remain above pre-pandemic levels.
- Workpuls: Daily pageviews averaged 1.9 million in December 2020, an increase of over 1000% between 2019 to 2020.
- Time Doctor: Received 5.9 million average daily pageviews in July 2020, up from 2 million in 2019. Time Doctor claimed to have 83,000 customers as of February 2021.

- ActivTrak: Daily average pageviews increased over 200% between 2019 and 2021, reaching a peak of 5.6 million in July 2020 and declining to 3.4 million in early 2021. ActivTrak claimed to be used by over 6,500 organizations as of February 2021.

- Teramind: Received 9.9 million daily average pageviews at its peak in July 2020, up 800% from a 1.1 million average in July 2019. As of February 2021, average daily pageviews fell to 3.9 million.
DATA and ALGORITHMS at WORK

The Case for Worker Technology Rights

By Annette Bernhardt, Lisa Kresge, and Reem Suleiman
UC Berkeley Labor Center
November 2021
## Contents

Overview ........................................................................................................................................ 1

Part 1: The New Workplace Technologies ..................................................................................... 4
  A brief overview of data and algorithms ..................................................................................... 4
  Industry examples of workplace applications ............................................................................. 6
  Potential harms for workers ...................................................................................................... 15

Part II: A Framework for Worker Technology Rights ................................................................. 18
  The regulatory vacuum ............................................................................................................. 18
  Towards a policy framework .................................................................................................... 19
  Principles .................................................................................................................................... 20
    1. Goals and Scope ................................................................................................................. 20
    2. Disclosure ........................................................................................................................ 20
    3. Worker Data ...................................................................................................................... 21
    4. Use of Electronic Monitoring ............................................................................................. 22
    5. Use of Algorithms ............................................................................................................. 23
    6. Discrimination ................................................................................................................... 23
    7. Organizing and Bargaining ................................................................................................. 24
    8. Impact Assessments .......................................................................................................... 25
    9. Enforcement ..................................................................................................................... 25

The Path Ahead ............................................................................................................................. 27

Endnotes ....................................................................................................................................... 29

References .................................................................................................................................... 34
Overview

Across the country, employers are increasingly using data and algorithms in ways that stand to have profound consequences for wages, working conditions, race and gender equity, and worker power. How employers use these digital technologies is not always obvious or even visible to workers or policymakers. For example, hiring software by the company HireVue generates scores of job applicants based on their tone of voice and word choices captured during video interviews. Algorithms are being used to predict whether workers will quit or become pregnant or try to organize a union, affecting employers’ decisions about job assignment and promotion. Call center technologies are analyzing customer calls and nudging workers in real time to adjust their behavior. And grocery platforms like Instacart are monitoring workers and calculating metrics on their speed as they fill shopping lists.

In these and many other examples, business operations and decisions are informed by near-constant collection and analysis of worker data. This trend toward data-driven workplaces has been exacerbated by the COVID-19 pandemic, with workers experiencing more invasive forms of monitoring, both inside the workplace (such as tracking social distancing behaviors) and in remote workers’ homes (such as keystroke tracking). And Amazon’s warehouse and delivery workers took the brunt of skyrocketing demands for delivered goods, with constant surveillance and productivity tracking software pushing the pace of work to an alarming rate and putting workers’ health at risk.

As a country we are finally talking about consumers and their technology rights, whether it’s about the data that social media companies are gathering and selling or the manipulation of elections via fake news postings. New policy responses are also starting to emerge. Consumer data privacy bills are proliferating at the state and federal levels, localities are banning the use of facial recognition technologies, and civil liberties groups are suing social network platforms over discrimination in ads targeted by race, gender, and age. The tech sector itself is engaging in debates about the ethics and regulation of artificial intelligence.

By contrast, despite the proliferation of “future of work” conferences and white papers, there has been almost complete silence in policy discussions when it comes to workers and their technology rights. This, despite the fact that workers currently have very little say about what data is collected on them, how employers are combining that data with algorithms to make decisions about them, and how these systems impact their jobs and livelihoods.
The almost complete lack of regulation means that there are strong incentives for employers to use digital technologies at will, in ways that can directly or indirectly harm workers. Similarly, developers are largely free to sell untested and faulty systems based on dubious science, exacerbating the potential harms against workers.9 Those harms can take the form of work intensification and speed-up; deskilling and automation; hazardous working conditions; growth in contingent work; loss of autonomy and privacy; discrimination; and suppression of the right to organize. Of particular concern is that workers of color, women, and immigrants can face direct discrimination via systemic biases embedded in these technologies, and are also most likely to work in occupations at the front lines of experimentation with artificial intelligence. A future where workers labor in digital sweatshops, micro-managed with no autonomy and under constant pressure, is not too difficult to imagine.10 This is already the reality for some workers.

In short, it’s time to recognize that workers have important and legitimate interests regarding the use of data and algorithms, just as consumers do. The discussion of technology rights needs to be extended into the workplace, explicitly confronting the fundamental imbalance in power between workers and the firms they work for—whether as employees, subcontracted workers, or independent contractors. Will data-driven technologies be used to benefit workers and enable them to thrive in their jobs? Or will technology be used to oppressively control labor, deskill jobs, suppress the right to organize, and reinforce race and gender inequality?

Public policy has a pivotal role to play in answering these questions. Technology is not inherently good or bad, but neither is it neutral; the role of workplace regulation is to ensure that technologies serve and respond to workers’ interests and to prevent negative impacts. Regulation is all the more important because employers themselves often do not understand the systems they are using. What we need, then, is a new set of 21st century labor standards establishing worker rights and employer responsibilities for the data-driven workplace. These standards should be established both in public policy, which is our focus here, and in collective bargaining agreements in unionized workplaces.

The goal of this report is to give policymakers and other stakeholders an understanding of trends in the data-driven workplace and a framework of the technology rights that workers need and deserve. In Part I, we describe data-based technologies, how they are being used in a wide range of industries, and the potential harms for workers.11 We then lay out in Part II a new set of policy principles that give workers rights with respect to their data; hold employers responsible for any harms caused by their systems; regulate how employers use algorithms and electronic monitoring; ensure the right to organize around technology; guard against discrimination; and establish a strong enforcement regime.

WORKER VOICES
A former warehouse worker, speaking about the stress of productivity quotas:

“I have anxiety just because I’m constantly scanning things, trying to be fast. They have this chart up that they would post after every break and it would show the number of items everyone was scanning and it would make everyone, it would make me feel like I had to hurry up or be faster. It gave me anxiety and physically wise, it was just moving fast to box faster or scan things faster.”
We view these technology rights and protections as the bedrock upon which to build an economy that works for everyone. Ultimately, the goal is that workers fully participate in decisions over which technologies are developed, how they are used in the workplace, and how the resulting productivity gains are shared. This participation need not and should not be anti-innovation, because workers have a wealth of knowledge and experience to bring to the table. Dehumanization and automation are not the only path. With strong worker protections in place, new technology can be put in the service of creating a vibrant and productive economy built on living wage jobs, safe workplaces, and race and gender equity.
Part I
The New Workplace Technologies

The revolution in big data and artificial intelligence of the past two decades has yielded a wide array of tools that employers can use to capture and analyze worker data, electronically monitor their workers, and manage them using algorithms. Of course, data analytics applied to work processes is not new; for example, Taylorism and scientific management formed the linchpin of mass industrialization. But today, we are seeing employers develop new business models and methods of worker control and productivity management based on digital systems that have the potential to substantially affect working conditions, job quality, and race and gender equity.

It is important to understand that the data-driven workplace is an emerging trend; we are just at the beginning of both the development and the adoption of these digital technologies. Moreover, the lack of regulatory oversight has turned workplaces into sites of experimentation with these systems, many of which are hidden from workers, policymakers, and researchers. That said, below we give a brief overview of data-driven technologies being developed for and deployed in workplaces, provide examples of applications in a range of industries, and identify potentially harmful impacts on workers. We draw on interviews with technology and labor experts, including workers, as well as technology vendor materials and extensive secondary research conducted by us and others.

A brief overview of data and algorithms

Data-driven technologies can range from the mundane (such as resume-parsing technologies that identify keywords and skills) to the incredibly complex (such as computer vision-based detection of human activities). Here we give a simple review of these technologies and how they are used.

Worker data collection: Employers can collect an extensive array of data about workers. Some of it is gathered in the workplace, such as computer activity, location in the building, customer ratings, bathroom use, coworker interactions, and smartphone app interactions. Other data is bought from third parties, like social media activity, credit reports, driving history, and consumer activity. Some of this data, such as criminal background checks, has been collected by employers for decades. More recently, as new wearable sensors have become available, employers have partnered with technology vendors and wellness programs to collect more personal biometric and health
and wellness data. Methods of data collection range from directly soliciting data from workers (and customers) through surveys or data mining the internet, to microphones embedded in worker badges. Employers may collect worker data themselves, but they may also contract with third-party firms to do so; an entire ecosystem is emerging of businesses engaged in collecting, processing, and selling worker data. New technologies continue to be developed at a rapid pace, expanding the range of worker data that can be captured.14

**Electronic monitoring:** Electronic monitoring is a particularly invasive form of data collection that entails extensive, and often continuous, monitoring of worker behaviors and actions. While not new, electronic monitoring has become more common with the development of passive data collection technologies such as sensors embedded in workplace equipment, devices, and wearables (e.g., wristbands) that can capture a wide range of data on worker location, activities, and interactions with coworkers. Likewise, systems that log keystrokes and capture screenshots enable employers to monitor computer and internet activity. Employers also use GPS technologies embedded in vehicles or in workers' personal smartphones to monitor their presence on job sites and track their locations while out in the field. More recently, sophisticated monitoring systems based on advances in computer vision and human detection are being used to analyze in real time video captured by workplace cameras.15

**Algorithms:** An algorithm, in its simplest form, is a set of rules in computer programming code for solving a problem or performing a task based on input data. Computers are able to complete tasks independently by following the instructions outlined by the algorithm. The simple version of an algorithm is like a cookbook recipe: the algorithm is simply following a set of commands dictated by the programmer for how to transform the ingredients (data) into a meal (an employer objective). But recent advancements in artificial intelligence research have resulted in much more complex algorithms. The more advanced versions of these algorithms accomplish tasks and make decisions by mimicking human capacities to reason, learn, and recognize visual objects, text, and speech. The key point to understand is that algorithms transform input data into technological outputs, which can take the form of everything from promotion recommendations and instructions for delivery drivers, to chatbots and semi-autonomous service robots that complete job tasks.16

---

**WORKER VOICES**

A former retail store worker, talking about the impact of scheduling software:

"Unstable scheduling means that you miss out on simple, joyful things in life. It also means taking public transportation at dangerous times. It's hard to even sleep regularly when your employer demands you work 2 p.m. to 11 p.m. and then 7 a.m. to 4 p.m. Recently, the company moved to the other extreme and schedules are now so fixed that they don't allow for the unpredictable human life events that come up. Asking for a schedule change is terrifying because management is willing to cut your hours all together."
Workplace applications: Employers use data collection, electronic monitoring, and algorithms for a wide range of functions and purposes in the workplace, including:

- **Human resource analytics**, such as hiring, performance evaluation, and on-the-job training. Hiring software is an especially important example, because employers are increasingly using it to partially or even wholly automate the recruitment, screening, and evaluation of job candidates—with substantial risk of bias and discrimination.\(^{17}\)

- **Algorithmic management**, such as workforce scheduling, coordination, and direction of worker activities. Productivity management systems are an especially important example, where employers use electronic monitoring and algorithms to closely track workers’ productivity, set quotas, and make consequential decisions such as discipline or firing based on performance metrics.\(^{18}\)

- **Task automation**, where some or even all tasks making up a job are automated using data-driven technologies. Examples are computer analysis of security surveillance footage, semi-autonomous service robots, and self-driving cars. One of the most common scenarios is partial task automation, where employers use technology to augment (but not replace) workers’ jobs, such as in the use of customer service chat bots in the retail industry.\(^{19}\)

It is important to understand that data-driven technologies are, in the end, creatures of their creators and users. Humans make decisions about the objectives, design, and implementation of these systems.\(^{20}\) In the workplace, employers decide if, when, and how to use electronic monitoring; which performance metrics to use; which management decisions or functions to automate; and whether to continue using productivity systems that are potentially harmful to workers’ bodies.\(^{21}\)

### Industry examples of workplace applications

In what follows, we give concrete examples of how data-driven technologies are being used in a wide range of workplaces. This is not a comprehensive inventory. Our goal is to illustrate the diverse ways that employers are using data collection, electronic monitoring, and algorithmic management, with a focus on industries that often pay low wages and depend on the labor of workers of color, women, and immigrants.

#### Call centers

While call center employers have monitored workers for decades, basic audio recordings of calls are increasingly being replaced by much more advanced monitoring and performance management systems.

**Remote monitoring**: Remote working in the pandemic has both highlighted the use of existing technologies to monitor workers and accelerated the adoption of new technologies. For example, Teleperformance, a call center company that provides remote call center services, uses webcams with a computer vision system that monitors workers at their computers and attempts to detect whether they are following company policies. If the system detects a work rule violation (such as non-work use of a mobile phone), it can send real-time notifications to a manager who can intervene...
and address the issue with the worker immediately. Multiple studies have documented the negative stress-related health effects of this intense level of electronic monitoring.\textsuperscript{22}

**Worker guidance and performance scoring:** One technology vendor, Cogito, designs technology systems intended to help call centers improve customer service and efficiency. Its system monitors, records, and analyzes conversations and other interactions between call center employees and customers. Based on an analysis of customer sentiment and call center worker behavior, the system provides real-time behavioral guidance to workers on a computer dashboard, coaching them to express more empathy, pace the call more efficiently, or exude more confidence and professionalism. Supervisors also have access to a dashboard that notifies them of problematic situations and provides a “customer experience score” based on the worker’s performance metrics such as call efficiency, sales conversions, and customer churn.\textsuperscript{23}

**Warehouses and distribution centers**

Warehouses and distribution centers have been early adopters of electronic monitoring and algorithmic management tools to manage inventory and staff.

**Productivity monitoring:** The warehouse industry is at the forefront of adopting automated labor management systems designed to increase worker speed and decrease error rates. These systems often rely on a granular level of electronic monitoring to set productivity quotas. Data collected from handheld or wearable product barcode scanners enable firms to track workers’ scan rates, errors, and lag time between scans (which can result in workers being penalized for too much time “off task”). These systems can also send performance notifications to workers nudging them to increase their pace or accuracy. In some systems, productivity scores can be shown in real time on video-game “leaderboards,” pitting workers against each other. Managers can monitor workers and receive reports on their productivity metrics. The systems can even send automated notices to human resources to fire workers for repeated low productivity scores.\textsuperscript{24}

**Task direction systems:** Another type of warehouse technology focuses on directing worker tasks, especially picking products to fulfill orders. Two examples of these systems are voice-directed systems and autonomous mobile robot picking carts (also known as “lead me” carts). Both systems use algorithms that perform a variety of tasks, from analyzing warehouse workflow to assigning tasks and optimal picking routes to individual workers. “Lead-me” carts direct workers from one warehouse location to another, setting the pace of work and instructing the worker on what product and quantity of items to pick at each stop. Voice-directed systems provide workers with verbal
step-by-step instructions on how to navigate the warehouse and which items to pick. Workers wear headsets with microphones and carry mobile devices equipped with speech recognition systems that enable workers to receive directions and verbally confirm task completion to the system. Both systems enable a granular level of monitoring of worker activities and provide managers with extensive data analytics on worker performance.25

Home care

As the U.S. population ages and demand for home care services for elderly and disabled people continues to grow, new technologies designed to monitor and manage home care workers are proliferating.

Electronic visit verification systems: In an effort to prevent fraud, the federal 21st Century Cures Act of 2016 included a provision requiring states to implement a system of electronic visit verification (EVV) for home care services reimbursed under Medicaid to ensure that services are actually rendered to those who qualify for home care assistance. The Cures Act requires that EVV systems provide a means to verify the date, time, location, and type of service provided, as well as the individuals providing and receiving the service. However, EVV implementation varies widely across states and in its degree of invasiveness for workers. In California, the home care worker is only required to enter relevant visit data into an online portal. Other states issue handheld devices, which the worker uses to clock in and out and record service data during the home care visit. Some states require workers to install an app on their smartphones that tracks their location in real time. In the most invasive version of EVV, states may also opt to include biometric recognition systems, such as facial recognition or fingerprints, to verify the identity of the home care worker or recipient.26

Home care apps: Two types of home care platforms—or apps—are increasingly being used in the industry: (1) on-demand platforms that manage the labor and payment transaction between a care provider and customer, and (2) marketplace platforms that provide a listing of available workers to individual households who then employ workers directly. On marketplace platforms, such as Care.com, clients can view worker profiles to find and select service providers. Worker profiles display performance metrics based on data compiled by the platform, such as customer request response times and customer ratings (which have the potential to perpetuate discrimination against people of color and immigrants in hiring and wage offers).27 These ratings have a significant impact on which workers will be featured in customers’ searches, and therefore on their likelihood of finding work.

WORKER VOICES

A nanny, talking about an online job matching platform and its lack of worker protections:

“There is always the assumption that a family seeking care must be given assurances that their loved ones are in safe hands, and they are given the option to select providers who have passed “rigorous safety checks.” However, there is very little impetus to consider that providers may very well also be someone’s loved one—how is their safety guaranteed? I have been in positions where I have felt sexually harassed, threatened, and humiliated by care seekers, yet there is no data trail available to alert other platform users to their behaviors. Is my safety and dignity less valuable?”

A nanny, talking about an online job matching platform and its lack of worker protections:
Retail and grocery

In addition to using technology to have customers do their own check-out, the retail industry is also at the forefront of using technology to collect data, monitor, and manage workers.\(^{28}\) Key examples include:

**Background checks and social media monitoring:** Large retailers often deploy hiring technologies to help process large volumes of job applications. One company, HireRight, offers services tailored to the retail industry. In addition to standard checks for criminal records, immigration status, and other background screenings, HireRight maintains a retail theft database of employer reports of employee shoplifting, theft, or fraud—包括 alleged thefts that never resulted in legal action. Despite multiple legal challenges, retail theft databases remain legal. Likewise, criminal background checks are often plagued with errors. Moreover, given the well-documented racial bias in the criminal justice system, even accurate background checks can perpetuate racial discrimination and labor market exclusion. HireRight also recently developed a partnership with a technology vendor specializing in data mining job candidates’ personal social media accounts, to predict the risk that job candidates may be whistleblowers. The same strategies have also been used to identify worker organizing activities.\(^{29}\)

**Workforce scheduling systems:** Over the past decade, many retailers have adopted scheduling optimization systems. These systems draw on a variety of data to predict customer demand, make decisions about the most efficient workforce schedule, and generate schedules that can adjust in real time as new data becomes available. Some systems, such as Percolata, use computer vision and algorithms to monitor and measure in-store customer traffic and worker activities. The Percolata system then estimates sales productivity scores for each worker and creates schedules based on those scores. Scheduling optimization systems can be programmed to incorporate worker preferences or to prevent back-to-back (“clopening”) or erratic schedules. However, these capabilities are often not fully enabled by managers and programmers, which can result in highly variable, unpredictable, and discordant schedules for workers.\(^{30}\)

**Grocery delivery apps:** One of the most substantial technological changes in the grocery industry over the past few years has been the introduction of order fulfillment and food delivery platforms. One of the largest, Instacart, allows customers to monitor and communicate with workers as they shop for and scan each item on the customers’ grocery list, receive notifications of estimated delivery times, and rate workers’ performance. The platform also tracks and generates metrics on the workers’ accuracy, speed in fulfilling orders, degree to which they follow scripted language in chat conversations with customers, as well as their customer ratings. Workers receive regular notifications regarding their performance and are penalized for not meeting speed and quality metrics, which can result in firing or removal from the platform.\(^{31}\) Another grocery platform app, Shipt, translates performance metrics into an “effort-based” pay algorithm that obscures how pay is calculated and has been shown to distribute pay inequitably among workers.\(^{32}\) It is important to note that grocery stores are themselves also adopting monitoring technologies (e.g., barcode scanners, computer vision systems, etc.) to evaluate and score the performance of their in-house workers.
Janitorial and security services

The building services industry is increasingly adopting workforce management systems that rely on cloud-based platforms and mobile apps to manage and track workers such as janitors and security guards.

**Janitorial services:** Many janitorial companies have turned to platform-based systems to manage their workers. These systems serve a wide range of functions, from allowing workers to view pay stubs and check work hours to requesting time off and completing training modules. Some systems enable workers to clock in and out for shifts, submit maintenance reports, and send and receive notifications to supervisors. More advanced systems rely on algorithms to optimize cleaning routes and assign job tasks to workers, and then require workers to scan QR codes to verify they’ve completed a task. Others may include GPS to track workers’ presence on a job site, detect rule violations (e.g., late check-ins), and send alerts to managers. GPS-based monitoring systems can easily extend employers’ ability to monitor workers well beyond the workplace and work activities.33

**Building security:** Building security companies are deploying similar platform-based management systems as the janitorial industry. Many of the functions are the same (e.g., human resources features, job task verification and monitoring). However, some security guard management systems also allow workers to report incidents by uploading time-stamped photos (with geolocation) or notes from their phone. More advanced systems rely on complex algorithms to analyze data collected through CCTV video cameras and building sensors and automate decisions about when to deploy frontline security guards. Some of these systems are designed to classify objects in the video stream (such as firearms) while other systems use facial recognition systems to identify potential shoplifters. This raises questions of responsibility and accountability, given that these systems are not error proof—i.e., will workers be blamed when the systems make an error.34

Transportation

Employers in the transportation industry use a wide range of technologies to monitor, manage, and direct workers who drive passengers or deliver goods.

**Driver monitoring:** Truck and delivery fleet drivers are subject to extensive electronic monitoring. For example, sensors in trucks track everything from location, braking and acceleration patterns to lane changes, speed, and seatbelt use. Additionally, dash cams and audio recording technologies monitor and collect data on driver activities in the truck cab. Increasingly, these data streams are further analyzed using computer vision systems along with facial analysis and object recognition techniques to identify driver fatigue or driver distractions, such as texting or eating while driving. These systems enable fleet managers to exert control over workers by setting quantified metrics to evaluate driver performance and challenge workers’ accounts of driving conditions.35

**Transportation platforms:** Transportation platform companies such as Uber and Lyft offer on-demand services to customers by dispatching drivers (typically misclassified independent contractors) to pick-up and drop-off locations and coordinating communications through their apps. Not only do the platforms handle payment between parties, they set the price of the service and receive a percentage of the transaction. The platform app enables the companies to manage workers
from afar, directing their activities, sending them notifications, and monitoring and collecting data on their behaviors. Moreover, the companies use incentives and penalties to shape worker decisions (e.g., when and for how long to drive). Drivers can be penalized for canceling or declining dispatches or for poor customer ratings, which in some cases can result in deactivation from the platform.\textsuperscript{36}

**Restaurants**

Although the restaurant industry has experimented with robots and other types of automation, customers still largely prefer human servers. Therefore, restaurants have turned to technologies that cater to customers and monitor staff performance.

**Self-service ordering:** Restaurants are increasingly installing tabletop tablets that allow customers to browse menus, self-order food, and pay at the table. Some systems connect the tabletop ordering system with wearables, such as watches, that enable staff and managers to receive real-time notifications of customer requests or complaints. At the end of the meal, these systems can also prompt customers to fill out a satisfaction survey to rate their experience and their server. Some systems translate customer ratings into a score that restaurants can use to evaluate servers, effectively shifting managerial evaluation to the customer. Research has shown that relying on customer ratings for worker performance metrics can facilitate harassment and perpetuate discrimination.\textsuperscript{37}

**Performance monitoring:** Another emerging technology in the restaurant industry is the use of electronic monitoring to analyze workers’ job performance. For example, the company Presto has developed a computer vision system that analyzes video data streams to automatically classify objects and human activities (and therefore flag, for example, long wait times for food or untidy waiting areas). The system uses this analysis to generate scores of likely customer experience. Based on these scores, the system can send real-time notifications to staff so that they can address issues immediately, as well as individual performance reports to managers. The company offers a similar product to monitor fast-food workers as they process orders for drive-thru customers; this system purports to identify worker errors and evaluate job performance. Not surprisingly, computer vision systems that classify human activities can easily produce inaccurate, unfair, or biased analyses, which, when coupled with algorithmic assessments of worker performance, can negatively impact workers.\textsuperscript{38}

WORKER VOICES

A restaurant waiter, speaking about the impact of online customer reviews:

“There was one time where a customer was upset because the food was taking forever and I kept checking with the kitchen and checking in on the table to apologize. They were rude but I was still professional and told them we were short staffed. But they left a really bad review on Yelp after and even named me. The manager spoke to me about it and didn’t give me the benefit of the doubt, even though I told him I can’t control how fast the food comes out of the kitchen.”
Hotels

The hotel industry has increasingly adopted a suite of technologies to monitor and manage front-line workers, especially housekeepers.

Worker safety: The hotel industry has begun to introduce “panic buttons” to protect hotel workers from sexual assault and harassment (largely as a result of legislation supported by unions and requirements of collective bargaining agreements). Panic buttons are devices that housekeepers and other isolated workers carry with them while working, which when activated will notify security or emergency personnel of the worker’s precise location. The buttons rely on technologies, such as Wi-Fi and GPS, and can vary from simple devices that transmit a signal only when activated, to more complex systems that enable continuous real-time location tracking. These features can be used by employers for purposes other than worker safety, such as collecting data on workers’ location that can be used to evaluate job performance. When these systems are not strictly regulated, they potentially expose workers to data privacy and security risks.39

Service optimization: Hotels are increasingly adopting service optimization systems that automate task prioritization and delegation. These systems are designed to achieve a specified management objective, room cleaning order, or personalized VIP services. When guests check out of their room or request services, the system automatically delegates the task to a worker based on criteria such as their proximity or workload. Through a smartphone or tablet, workers receive notifications and an ordered task list, which can change in real time throughout the day. Managers can also access the system to communicate with workers, manually delegate tasks, and monitor workers’ activities. These systems can lead to incoherent task prioritization, unrealistic productivity expectations, and work intensification for jobs that are already physically demanding and prone to injuries.40

Health care

The COVID pandemic has prompted a profound revolution in health care with the expanded use of telehealth, but other technologies impacting workers have been introduced as well.41

Hand-hygiene monitoring: Hospitals are increasingly using automated hand-hygiene compliance monitoring (HHCM) systems to monitor workers’ handwashing behaviors. The most advanced systems use sensors and wearables (e.g., badges) to link soap or sanitizer use with workers’ entrance or exit in rooms or their proximity to patients. Some systems alert workers in real time (via color-coded lights, wristband vibrations, etc.) if the system detects non-compliance with handwashing protocols (e.g., did not wash hands long enough). Alternatively, some systems provide
positive feedback to workers on their compliance. HHCM systems can allow managers to view data in real time and generate handwashing performance reports at the department, team, or individual level. But studies have questioned the accuracy of some of these systems and raised concerns for their validity in measuring compliance, which could result in unfairly disciplining workers.42

**Service robots:** Health care industry adoption of semi-autonomous robots is on the rise and appears to be accelerating with the COVID pandemic. For example, workers use delivery robots, or “smart carts,” to transport materials (e.g., linens, meals, lab specimens) to other workers. Floor cleaning robots vacuum or scrub floors along a preset route programmed by workers, who also monitor and support their operation. Semi-autonomous robots rely on a variety of technologies—such as Wi-Fi, cameras, lasers, infrared and ultrasonic sensors, and GPS—to navigate hospital corridors and avoid human and nonhuman obstacles. Unlike algorithmic systems that monitor and make decisions about workers, service robots rely on algorithms to navigate their physical environment and work alongside workers. Importantly, hospital staff must be trained on how to work around robots and support their functioning in the complex hospital environment. This raises questions of responsibility and accountability, given that workers often take the blame for automation failures.43

**Construction**

The construction industry has incorporated technologies that can monitor workers’ locations on job sites, and scan for safety hazards to prevent injuries on the job.

**Location monitoring:** The construction industry is increasingly adopting workforce management systems that rely on geofencing and geolocation technologies. Geofencing software works by setting a virtual boundary around an area using GPS coordinates and detects when a mobile device crosses that boundary. These systems operate through apps installed on workers’ mobile phones that can tap into the phone’s GPS function and automatically clock workers in and out as they enter and exit the job site. Construction companies can also use these systems to track travel times between job sites or location histories of where workers traveled throughout the day. Managers can access a dashboard with real-time tracking data and receive alerts, such as workers clocking in outside of a designated job site.44

**Safety monitoring:** Safety monitoring systems are gaining momentum in the construction industry. Construction firms are increasingly using computer vision and complex algorithms to analyze video footage and classify whether workers are compliant with safety protocols (e.g., wearing proper personal protective equipment). Some companies have adapted these systems to detect workers’ compliance with COVID-19 protocols, like social distancing or mask wearing, and then send real-time alerts to workers and managers. Other companies have designed systems that focus on preventing accidents, for instance, by tracking workers as they walk through job sites and predicting in real time whether their trajectory places them at risk of being hit by heavy machinery. If the system determines a likely accident, it will alert the worker through vibrations on a wristband and disable the equipment to avoid possible injury.45
Public sector

In an effort to streamline and improve access to governmental services, and to manage an uncertain budgetary environment, the public sector is adopting new technologies that have important implications for its workers and their jobs—including teachers, social workers, and customer service agents.

**Automated benefit application support:** Government agencies handle a high volume of customer contacts, most commonly for benefit program applications and for inquiries (e.g., benefit eligibility). In the past, workers reviewed paper applications or computer forms. However, agencies are increasingly adopting a variety of technologies to keep up with the growing volume of benefit applications and inquiries. For example, some agencies have turned to chatbots or virtual assistants that use natural language processing technology (similar to that found in Apple’s Siri or Amazon’s Alexa) to answer simple questions or help people navigate applications. Other systems automatically process and review digital benefit program applications entered through phone apps or websites. Due to the large volume of work, these systems have typically not reduced jobs, but instead have resulted in workers handling more complex calls the system is unable to navigate. This shift can lead to work intensification and burnout, particularly if training is inadequate and workload measures do not reflect the changing level of complexity.46

**Automated decision-making tools:** Some government agencies have adopted or piloted technologies that automate decision-making for social services. Agencies are adopting these systems for two reasons: (1) to address concerns about bias or inefficiency in human decision-making, and (2) to help prioritize large caseloads when there is limited staffing. For example, agencies have adopted decision-making algorithms to identify priorities for investigations, such as responses to child protective services reports or domestic violence calls. While these technologies may replace some of the decisions previously made by humans, they can also free up social workers’ time, allowing them to focus on directly working with families. Many of these systems have received attention from scholars and advocates concerned about algorithmic harms against the public, especially in low-income communities and communities of color. However, a growing body of research also points to potential risks that these systems can pose for workers, such as loss of discretion in decision-making and being held responsible for negative outcomes for clients.47

**A note on COVID**

In some industries, the coronavirus pandemic has accelerated the adoption of data-driven technologies. An obvious example is electronic monitoring of social distancing behaviors to prevent the spread of the virus. Related, some companies added new features to existing worker management software, such as time-clock apps with “touchless” facial recognition features. Another example comes from the sudden and significant shift to remote work, which prompted increased use of webcams and other tracking software to monitor workers’ productivity more closely while working from home. Many restaurants and retailers have added delivery or curbside pick-up options, using third-party online ordering and delivery apps. And when shelter in place orders relaxed and hiring started again, many employers turned to virtual recruiting technologies, such as video interviews and algorithmic systems, to parse through applications and rank job applicants.48 It is too early to assess how much of this technology adoption will become permanent, but the pandemic clearly introduced many employers to the power of data and algorithms.49
Potential harms for workers

Currently, much of the policy discussion about data rights is focused on privacy concerns, in part because the main focus has been on consumers. But with the advent of flawed systems based on faulty data and pseudoscience and powerful technologies such as facial recognition, there is growing understanding that the potential harms of new technologies extend far beyond privacy. This is very much the case for workers, given the diverse set of hiring, management, and monitoring tools based on data and algorithms reviewed above.

We are only beginning to understand the full range of possible negative impacts on workers. Note that these harms are not inevitable; data-driven technologies can also be used to help workers, make them safer, reduce monotony, and improve their work lives. But first and foremost, the goal of public policy should be to prevent harms to workers, which include but are not limited to the following:

**Discrimination**

So far, the harm for workers from data-driven technologies that has been best documented is discrimination based on race, gender, age, disability, and other categories, especially in hiring software. The classic scenario is a hiring algorithm that is trained to look for job candidate characteristics that match a company’s current workforce, inevitably replicating the demographics—often white and male—of that workforce. But importantly, women and workers of color may also be disproportionately subject to harms from data-driven technologies because of the occupations where they work, especially low-wage jobs like warehousing and call centers where experimentation with invasive monitoring or algorithmic management is more likely.

**Work intensification and health and safety harms**

One of the key applications of data-driven technologies is to monitor and manage worker productivity, which is not harmful in and of itself. But when an employer uses technology to minutely track and relentlessly push workers to achieve greater productivity, the negative effects can quickly make themselves felt. Work intensification can have direct impacts on workers’ physical health and safety, as evidenced in the high injury rates that have been documented in Amazon’s warehouses. Moreover, electronic monitoring to closely track workers’ every move can significantly affect their stress levels and mental health. Extensive research has also linked job-related stress to ulcers, cardiovascular disorders, and other negative physical health consequences for workers.

**Deskilling and job loss**

Data-driven technologies can be used to routinize jobs and break them into discrete simplified tasks, accompanied by measuring and monitoring of performance. While the employer’s main goal may be to increase efficiency, the result for workers can be deskilling of their jobs, narrowing the scope of their work, and increasing repetition. The downstream consequences can be significant, in the form of lower wages, less access to training (since the job has been deskilled), and decreased job mobility. Depending on the industry, task standardization can then in turn also lead to partial or wholesale automation of those jobs, since the data gathered in real time on workers performing each task
can then be used to train robots or algorithms to eventually take over. For example, chatbots learn by example as they listen in on call center agent calls, and algorithms to be used in autonomous vehicles learn from hours of monitoring truck drivers.55

**Lower wages and less economic mobility**

Data-driven technologies can affect workers’ wages through multiple routes.56 Some can be direct—for example, when a job candidate is disqualified by an automated hiring system using criteria that are not obviously related to job performance and/or that tend to disfavor workers from marginalized groups. Wage theft is another direct example, as when time keeping software automatically deducts breaks (even if workers aren’t able to take them), or when intense productivity quotas discourage workers from taking the paid rest breaks they are legally entitled to.57 Other times the effects on wages can be more indirect. For example, when a job is deskilled and routinized by advanced technologies, it is effectively turned into a dead-end job. In a similar vein, an algorithmic management system may make recommendations to an employer about job assignments or promotions in ways that hurt the long-term career mobility of a worker. Data-driven technologies can also indirectly serve as gatekeeper to the labor market, if qualified workers have limited tech literacy or lack access to broadband internet.58

**Contingent work**

As new technologies enable remote monitoring and management of workers, the incentive for employers to outsource previously in-house jobs to subcontractors, staffing agencies, or platform-based work is high—and with it, the increased likelihood of misclassifying workers as independent contractors. A key reason that employers outsource is to avoid bearing the full costs of employing workers directly, such as having to pay the minimum wage, carry workers’ compensation, and provide health insurance and retirement benefits. Meanwhile, workers who depend on platform-based income are excluded from workplace protections and bear the brunt of job insecurity.59

**Suppression of the right to organize**

There are growing reports that employers are using surveillance technologies to identify workers who are trying to organize a union, as well as predictive algorithms (that data-mine social media) to identify workers who might be likely to try to organize one.60 Likewise, companies that design hiring systems can incorporate methods to screen out workers who are likely to be sympathetic to unions.61 Such attempts to identify organizing activity are in and of themselves an intrusion on the right to organize, but especially so when employers then take steps to stop the organizing or forestall it by firing or otherwise intimidating workers.62
Loss of privacy

Workers have significant privacy concerns in their workplaces. Electronic monitoring, for example, can easily stray outside of the workplace, via systems that scan social media activity or apps downloaded on workers’ phones that access GPS location data regardless of whether they are on the job. The risk is that this type of intrusive surveillance uncovers information about workers (e.g., their religion or sexuality) that is intensively private and not at all relevant to work performance. It may reveal a worker’s disability or other sensitive or legally protected information about the worker. Such intrusions into workers’ personal lives are especially likely for the growing number of people who are working remotely from their homes, given the broad data capture that is enabled by time clocking software or wearables that collect and use biometric data.

Loss of autonomy and dignity

Finally, workers stand to lose their autonomy and dignity when data-driven technologies are used to micromanage and monitor every activity and remove all room for discretion on the job. While not as immediate or concrete as some of the harms discussed above, the danger of dehumanization at work in the era of artificial intelligence is very real, and already being reported by workers. A visceral example is the potential public humiliation from having one’s productivity score compared to that of other workers on leaderboards. But ultimately this is about lost opportunities. Workers want and deserve to have agency in troubleshooting and innovating best practices and learning new skills; the quashing of that very human desire is part of what’s at stake in the debate about new technology.
Part II
A Framework for Worker Technology Rights

The emerging suite of data-driven technologies in the workplace raises critical questions. Will these technologies be used to benefit and empower workers, help them thrive in their jobs, and bring greater equity to the workplace? Or will they be used to deskill workers, extract ever more labor, increase race and gender inequality, and suppress the right to organize? Who is going to be at the table when these decisions are made, and in particular what role will workers themselves have? In other words, who is going to govern technology? And what values will we as a society choose to prioritize in that governance?

The regulatory vacuum

The cornerstone of governing workplace technologies will be laws and regulations (and collective bargaining agreements in unionized workplaces). But currently, employers are introducing untested data-driven technologies with almost no regulation or oversight. Workers largely do not have the right to know what data is being gathered on them or whether it’s being sold or shared with others. They don’t have the right to review or correct the data. Employers aren’t required to notify workers about electronic monitoring or algorithms that they’re basing decisions on, and workers don’t have the right to challenge those decisions. And currently, there are virtually no meaningful guardrails on which technologies employers can use and how they use them.

The United States lags significantly behind the European Union in regulating data-driven technologies. For example, the EU has already passed a wide-ranging data privacy law and is in the process of drafting a comprehensive artificial intelligence law. In the U.S., only a few scattered data privacy laws have been passed at the state level, all focused on consumers. And while recently we’ve seen a plethora of privacy bills emerge at the federal level, the timeline to actual passage will be long.

Meanwhile, a slew of legal analyses of existing employment and labor laws have concluded that they are wholly inadequate to the task of protecting workers in the data-driven workplace. In some cases, new laws will need to be written from scratch to, for example, establish a general...
right to worker privacy or establish guardrails on the use of algorithms.70 Similarly, employers’ electronic monitoring of workers is largely unregulated in federal law. Some states have scattered privacy protections for some workers, but these are typically focused on specific types of data (e.g., biometrics) or simply institute a weak notice and consent model (e.g., when employers monitor worker communications).71 In other cases, existing laws need substantial updating for the data-driven workplace. This is the case for anti-discrimination laws if they are to meet the challenge of addressing discriminatory harms stemming from algorithmic hiring and promotion tools.72 Similarly, our health and safety laws do not have sufficient standards to protect workers from the psychological stress, repetitive motion, and fatigue-related injuries that can result from productivity monitoring systems.73

Towards a policy framework

In short, we need a new set of 21st century labor standards establishing worker rights and employer responsibilities for the data-driven workplace. For the majority of workers who are not members of unions, the profound asymmetry of power in the U.S. workplace means they have little to no say over the policies and decisions that affect them in their day-to-day work lives.74 In particular, notions of consent to new technologies or the ability to find better conditions elsewhere are not meaningful or available to low-wage workers, women, and workers of color, who face a labor market that is often dominated by employers competing on the basis of cutting labor costs.75 Employment and labor laws have long attempted to balance this asymmetry of power by instituting baseline labor standards and giving workers a mechanism for voice; those laws need to be strengthened and updated for the 21st century workplace and its technologies.

In what follows, we outline a set of policy principles that can help build a robust regulation regime. The principles lay out a vision for labor standards that give workers rights with respect to their data; hold employers responsible for harms caused by their systems; regulate the ways in which employers monitor workers and use algorithms; ensure the right to organize around technology; guard against discrimination; and establish a strong enforcement regime for worker recourse.

These principles are intended to inform policymakers and worker advocates developing legislation at the federal, state, and local levels. The principles draw on proposals and policy concepts developed by lawyers, academics, and worker advocates in the U.S., Europe, and elsewhere.76 They include regulations of the technologies themselves as well as rules about when, how, and for what purpose employers use them in the workplace.
Importantly, we argue that new labor standards for digital technologies should first and foremost be embedded in employment and labor laws. Consumer-focused laws are insufficient for fully protecting workers because they are largely focused on privacy—and as described above, workers’ concerns about new technologies extend far beyond privacy to include impacts on wages, health and safety, working conditions, job stability, and race and gender equity.77

**Principles**

1. **Goals and Scope**

   The rapid pace of innovation in the use of data collection, electronic monitoring, and algorithms affects every stage of the employment lifecycle and requires broad, ambitious standards set in law. Full coverage of both workers and employers should be the governing principle, as should attention to the full range of potential harms for workers. Specifically:

   New rights and protections should be established to ensure worker dignity and welfare in the use of data-driven technologies in the workplace. These standards should be established in employment and labor laws. They should give workers agency over new technologies, promote health and safety, protect the right to organize, and guard against discrimination and other negative impacts.

   **All workers deserve protection.** New rights and protections should cover all workers, including employees, independent contractors, job applicants, and remote workers. Representatives from unions or other worker organizations should be able to access these rights and protections on behalf of workers.

   **All employers should be held to these standards.** Employers’ obligations should also apply to their labor subcontractors, as well as to vendors that provide technology or technology services.

   **All employment-related decisions that are made or assisted by data-driven technologies should be regulated.** Employers make a wide range of decisions based on digital technologies. These decisions should be regulated whenever they impact workers, including effects on earnings, benefits, hours, and work schedules; race and gender equity; hiring, firing, promotion, discipline, and performance evaluation; job assignments, job content, and productivity requirements; workplace health and safety; and the right to organize.

2. **Disclosure**

   Full disclosure and transparency are prerequisites for effective regulation. But currently, the biggest obstacle to regulating data-driven technologies is that their use is largely hidden from both policymakers and workers. Without disclosure, job applicants won’t know why a hiring algorithm rejected their resume; truck drivers won’t know when they are being tracked by GPS; and workers won’t realize their health plan data is being sold. Therefore:
Employers should provide notice to workers in a clear and accessible way regarding all data-driven technologies in the workplace. Notices should include an understandable description of the technology, the types of data being collected, and the rights and protections available to workers. Employers should also be required to file notices with the relevant regulatory agencies (i.e., those enforcing wage and hour, health and safety, and anti-discrimination laws).

Additional notification should be required when electronic monitoring is being used. This should include a description of which activities will be monitored, the method of monitoring, the data that will be gathered, the times and places where the monitoring will occur, and the purpose for monitoring and why it is necessary. Notice should also document how employment-related decisions could be affected.

Additional notification should be required when algorithms are being used that affect workers’ jobs or working conditions. This should include an accessible description of the algorithm, its purpose, the data it draws on, the type of outputs it generates, and how the employer will use those outputs in their decision making.

3. Worker Data

Employers can collect or buy vast amounts of data on their workers, and share it or sell it without restriction. It’s not realistic to expect workers to police that data collection themselves. Just like consumers, workers deserve legal standards on employers’ collection and use of their data, as well as more control over their personal information:

Employers should only collect worker data when it is necessary and essential for workers to do their jobs. Employers should minimize their collection of worker data, which should be defined broadly to include personal identity information, biometric and health information, any data related to workplace activities (including productivity data and algorithmic inferences), and online information including social media activity. Unlimited collection of their data unnecessarily exposes workers to risk, including data breaches and employers’ misuse of personal information.

Workers should have the right to access, correct, and download their data. Workers should receive all relevant information regarding their data, including why and how it was collected, if it was inferred about the worker, and whether it was used to inform an employment-related decision, including hiring. Employers should be responsible for timely correction of any inaccurate data.

Worker data should be safeguarded and protected from misuse. In particular, employers should not be allowed to sell or license worker data to third parties under any circumstances; otherwise, the incentives to violate worker privacy by selling worker data for monetary gain are too high. Individual workers’ biometric and other health data should never be shared unless required by law.
4. Use of Electronic Monitoring

Electronic monitoring is a highly invasive technology because it allows for real-time and continuous capture of worker activities and behavior. As a result, the potential for misuse of electronic monitoring by employers is high—for example, in violating workers’ privacy, in using biased or incomplete monitoring evidence to discipline someone, or in pushing the pace of work to the point of injuries. Therefore:

Employers should only use electronic monitoring for narrow purposes that do not harm workers. Electronic monitoring should only be used if strictly necessary to enable core business tasks, to protect the safety of workers, or when needed to comply with legal obligations. To minimize potential exposure and harm to workers, monitoring should affect the smallest number of workers possible, should collect the least amount of data necessary, and should be the least invasive means for accomplishing its purpose. Productivity monitoring in particular should be subject to higher scrutiny and reviewed by regulatory agencies overseeing workplace health and safety to ensure it is not used to speed up work to dangerous levels.

Employers should respect workers’ privacy in using electronic monitoring. Intrusive surveillance in the workplace, especially by audio and video, can capture information about workers that is private and not relevant to performance. Workers should not be monitored in the breakroom, sensitive areas like the restroom, or off duty. Any GPS or other tracking devices should be disabled when the worker is off the job.

Electronic monitoring should not use high-risk technologies such as facial recognition. Some new monitoring technologies are too risky to introduce in the workplace; for example, facial-recognition systems have been documented to have high error rates and racial bias. Employers should be prohibited from incorporating unproven, questionable, or particularly invasive technologies into their electronic monitoring systems.

Electronic monitoring should not be used as a substitute for human decision making. Even in the best cases, electronic monitoring systems can only capture a partial picture of a given event or set of actions; in the worst cases, that picture is misleading or wrong. Employers should therefore be prohibited from relying exclusively or even mainly on data from electronic monitoring when making consequential decisions like hiring, firing, discipline, or promotion. Instead, employers should be required to conduct independent, human-driven assessments of workers based on other information sources.

Workers should be given full documentation when an employer makes a consequential decision informed by electronic monitoring. Workers should also be able to challenge that decision.

WORKER VOICES

A school bus driver, talking about the impact of security cameras on buses:

“The bus cameras are the worst—they were originally installed to protect the kids, but now three cameras are pointed directly at us and recording at all times, even when no kids are on the bus. We know now that they use this footage in personnel matters, they listen to us through the bus cameras, and that they use the cameras to read our text messages when we are parked and using our phones while the children are off the bus and we are on breaks from work.”
5. Use of Algorithms

The explosion in algorithmic management tools creates significant risk for workers; many of these technologies are opaque, untested, and being used by employers with little attention to or understanding of their potential harms for workers. The stakes for workers are simply too high when decisions like hiring and firing are about being made about their lives. Therefore:

**Employers should not use algorithms that harm workers’ health, safety, and wellbeing.** Employers should be responsible for ensuring that any employment-related decisions assisted by an algorithm are fair, reasonable, and do not harm workers, in part by conducting an impact assessment prior to adoption of the algorithm. Productivity algorithms in particular should be subject to higher scrutiny and reviewed by regulatory agencies overseeing workplace health and safety for potential harms.

**Employers should not use algorithms to make irrelevant or unfair predictions about workers.** The marketplace has seen a spate of pernicious “snake oil” algorithms making what turn out to be unsubstantiated predictions about workers. Employers should be prohibited from making predictions or inferences about a worker’s traits and behaviors that are unrelated to their job responsibilities. Similarly, employers should not be able to use algorithms to predict or make judgements about a worker’s emotion, personality, or health.

**Employers should not use high-risk algorithmic technologies such as facial recognition or expression analysis.** Employers should be prohibited from using algorithms that incorporate unproven, questionable, or particularly invasive technologies.

**Algorithms should not be used as a substitute for human decision making.** The growing complexity of algorithmic systems means that even their developers may not understand how they arrive at conclusions—let alone the employers deploying these systems. Employers should therefore be prohibited from relying exclusively or even mainly on algorithms when making consequential decisions like hiring, firing, discipline, or promotion. Instead, humans should have a substantial and meaningful role in the decision, drawing in other sources of information. Human decision makers should be trained to understand what a particular algorithm does and the limitations of its output.

**Workers should be given full documentation when an employer makes a consequential decision assisted by an algorithm.** Workers should also be able to challenge that decision.

6. Discrimination

Growing evidence suggests that data-driven technologies carry significant risks of discriminating against workers on the basis of race, gender, age, disability, and other characteristics. The “black box” nature of many of these technologies—and their use for consequential decisions such as hiring and promotion—means that regulatory scrutiny needs to be especially high. The following is adapted from “Civil Rights Principles for Hiring Technologies,” expanded to the full range of workplace applications.
Data-driven technologies should not discriminate against workers based on protected characteristics. Policymakers should make clear that anti-discrimination laws apply to all workplace data-driven technologies. In particular, the use of data-driven technologies with a disparate impact should trigger the same level of scrutiny as any other discriminatory employment practice.

Removing protected characteristics from data-driven technologies should not give employers a free pass. The fact that an employer does not use protected characteristics such as race or gender in its algorithm or data system does not mean that the technology cannot have a disparate impact. Employers should still be required to test for disparate impacts and mitigate any harms.

Policymakers should update existing regulations on worker assessment tools. Data-driven technologies in worker assessment tools should only measure traits that have a logical and explainable relationship to the job at hand. They should not use mere correlation to make judgements, inferences, or predictions about a worker’s or job applicant’s ability to perform the job.

7. Organizing and Bargaining

Across the country, especially in low-wage industries, workers are increasingly voicing their frustration with excessive monitoring and algorithmic management in their workplaces. They should be able to organize around these issues without retaliation, and, when represented by unions, be able to bargain over them. Specifically:

Labor organizations should have the right to bargain over employers’ use of data-driven technologies. Federal labor law requires employers to bargain with worker representatives over the terms and conditions of employment. Data collection, electronic monitoring, and algorithmic management all impact the terms and conditions of employment. Unions should have access to the information necessary to fully understand the nature, scope, and effects of data-driven technologies used by the employer, and the employer should be required to bargain in good faith over them.86

Even when they are not represented by a union, workers should have the right to organize around the use of data-driven technologies in their workplace. When workers protest a company’s collection of their data, question the decisions made about them by algorithms, or seek to learn more about data practices, labor laws should be understood to protect this collective activity.
Employers should not use digital technologies to identify, monitor, or punish workers for organizing. Monitoring workers who are engaging in organizing activities has long been held to violate the law for its chilling effects. Employers should not engage in surveillance of workers when they are meeting with union representatives or discussing workplace problems. Efforts to screen workers using electronic monitoring or predictive algorithms for their sympathy with unions should also be recognized as illegal.

8. Impact Assessments

The novel and inscrutable nature of many data-driven technologies means that their impacts on workers are not self-evident. But waiting to discover harms after an algorithm or data system has already been implemented is not fair to workers. These technologies should be thoroughly vetted and made safe for the workplace before they are introduced. Specifically:

Data-driven technologies should be continuously evaluated and harms mitigated. Employers should be required to audit their technologies by conducting rigorous impact assessments, both prior to implementation and throughout the lifecycle of the technology. They should be required to address any risks that are identified and be held legally liable for any harms caused by their technologies. Employers should also be required to submit impact assessments to the relevant regulatory agencies, which should have the right to halt the use of harmful systems.

Impact assessments should evaluate the full range of potential harms to workers. These include discrimination, harms to mental and physical health and safety, loss of privacy, and negative economic impacts.

Workers should have a role in impact assessments and have the ability to challenge them. Workers have significant and useful knowledge about a company’s production processes and how technology actually works on the ground. They (and their unions) should be consulted in all stages of an impact assessment and be able to review and give feedback. They should also be able to dispute the final assessment with the relevant regulatory agencies.

9. Enforcement

Enforcement is the lifeblood of laws and regulations; without it, the promise of legal rights is hollow. This is especially the case when it comes to the use of data-driven technologies, where the asymmetry of power and information between workers and employers is pronounced and where the incentives for employers to misuse opaque technologies are strong. Specifically:

Regulatory agencies should play a strong role in enforcing workplace technology standards. Workers should be able to submit complaints about employer noncompliance to regulatory agencies (i.e., those enforcing wage and hour, health and safety, and anti-discrimination laws). In turn, those agencies should respond to each complaint, apply penalties when warranted, and initiate workplace-wide investigations when needed. Regulatory agencies should also have the authority to proactively audit employers’
use of data-driven technologies. When technologies are found to harm workers, agencies should have the authority to require that employers mitigate the harms or halt the use of systems that can't be made safe.

**Regulatory agencies should have the authority to establish additional rules and standards.** This allows the agencies to respond to rapid developments in existing and new technologies introduced in the workplace.

**Workers should have a private right of action to sue employers for any violations of their technology rights and protections.** The right for workers to sue their employers is a central pillar of robust enforcement, allowing them to control their own case and complementing agency enforcement efforts. Employers should also be prohibited from retaliating against workers for enforcing their rights.
The Path Ahead

In this report, we have argued that the arrival of data-driven technologies in the workplace poses significant risks to workers and requires the creation of a new set of labor standards in employment and labor laws. These new standards must be bold, comprehensive, and continuously updated to respond to the rapidly changing terrain of workplace technologies and the potential harms that workers face from them.

But while worker data rights and protections are critical, they alone will not be enough. For example, workers should receive the training needed to grow with their jobs and participate fully in technological change. Government staff need the skills and adequate resources to provide oversight and enforcement. Public R&D funding should be leveraged and increased to incentivize the development of technology that benefits people and the planet. The public sector itself must become a model for accountable technology adoption. And the U.S. must build out a robust governance regime of regulating the designers, developers, and producers of new workplace technology. Above all, workers and their communities—especially low-income communities, women, immigrants, and communities of color—must be included in the development of that governance regime; their knowledge and experiences will be the keystone to ensuring that innovation truly contributes to the social good.

WORKER VOICES

A warehouse worker, speaking about the abundance of surveillance in the facility:

“I hate it. I hate the fact that a lot of the technology is really about surveillance and keeping tabs on somebody and controlling everything that they do. And I just really have a huge dislike for that. I don’t think it’s right. I think it gives the wrong impression, too. Makes everyone that works there feel like a thief. So that’s not a good feeling to walk into a job where you feel like you’re being called a thief.”
Acknowledgements

This report has been deeply informed by an inspiring community of researchers, lawyers, journalists, and advocates focused on documenting and analyzing the impact of new technologies in the workplace. We are especially grateful to the workers, unions, and other worker organizations who shared their experiences with us, and to the participants of a working group in California that contributed significant expertise to the development of the policy principles presented here. We thank the multiple reviewers of this report for their invaluable feedback. This report was generously supported by grants from The James Irvine Foundation and the Ford Foundation. Finally, we want to give a special thanks to Emlyn Bottomley for his invaluable contributions to the initial stages of this project and to our team. All errors of fact or interpretation remain our own.

This report is licensed to the public under a non-exclusive Creative Commons Attribution 4.0 International (CC by 4.0) license, https://creativecommons.org/licenses/by/4.0/.

About the Authors

Annette Bernhardt is director of the Technology and Work Program at the UC Berkeley Labor Center.

Lisa Kresge is a lead researcher for the Technology and Work Program at the UC Berkeley Labor Center.

Reem Suleiman is a policy researcher for the Technology and Work Program at the UC Berkeley Labor Center.
Endnotes

1. Throughout this report we use the terms “digital technologies” and “data-driven technologies” interchangeably when referencing the wide range of technologies that gather and transform data into outputs such as rankings, predictions, decisions, and machine-based actions.

2. For a description of HireVue’s hiring technology system, see Aspan (2020). HireVue’s initial system used expression analysis technologies to assess job candidates, which they have since discontinued due to growing concern from technologists, academics, and civil rights advocates about the validity of their system (see Maurer 2021b).

3. For information about “flight risk” algorithms that attempt to predict whether workers will quit, see Liu (2019). Also, Hao (2020) describes a tech vendor that attempts to predict whether job candidates are likely to quit before they are hired. See Zarya (2016) regarding employer efforts to predict pregnancy and Kessler (2020) regarding employers attempting to predict union organizing.


5. See Bhuiyan (2020) for more information about how grocery platforms, such as Instacart, operate.


7. See Kantor, Weise, and Ashford (2021).

8. Greenhouse (2019) discusses the absence of workers in “future of work” discussions. Also, Gupta, Lerner, and McCartin (2018) point out that “future of work” discussions often assume a narrow vision of technological change and a future of work without workers, which leads to policy solutions focused on ensuring basic survival; they argue that the discussions should focus instead on the future of workers and how innovative technologies can contribute to a humane and sustainable future. Townsend (2021) argues that data protection policies need to recognize all aspects of individuals’ lives and extend consumer data rights to workers.

9. For a discussion of “AI snake oil,” see Narayanan (2019), and see Slaughter (2021) for an overview of how algorithmic systems can cause harm.

10. For an overview of how algorithmic systems can be used to control workers, see Kellogg, Valentine, and Christin (2020). Also, see Cappelli (2020) for a discussion of the recent shift toward Taylorist management models enabled by extensive worker monitoring and algorithms designed to control workers.

11. For other excellent research overviews, see Adler-Bell and Miller (2018), Bogen and Rieke (2018), Milner and Traub (2021), Nguyen (2021), Scherer and Brown (2021), UNI Global (n.d.), and Zickuhr (2021).

12. For a deeper treatment of data collection, electronic monitoring, and use of algorithms in the workplace, see Briône (n.d.) and Kresge (2020). Also, see Bogen and Rieke (2018) and Reike et al. (2021) for an overview of data and algorithms in the hiring process.

13. See O’Connor (2016) for a description of Taylorism and scientific management. See Davenport (2018) for a description of the transition from business (workplace) data analytics to artificial intelligence.

14. For an overview of the data collection in the workplace, see Alder-Bell and Miller (2018) and Kresge (2020).


17. For an overview of technologies used in the hiring process, see Bogen and Rieke (2018).

18. See Ajunwa (2018) for an overview of productivity monitoring systems in the workplace. Kaplan (2015) describes various workplace monitoring systems used to manage workers. Also, see Kellogg, Valentine, and Christin (2020) for a discussion on the use of algorithms to discipline workers. Amazon has received the most attention for their productivity management systems based on algorithms; for example, see Lecher (2019). Another notable example of algorithmic management driven by productivity metrics is Instacart; see Griesbach et al. (2019) and Bhuiyan (2020).

See Luca, Kleinberg, Mullainathan (2016) and Frankowski (2019) for a discussion about the role of humans in shaping the objectives and design of algorithmic systems.

See Cappelli (2020) regarding management strategies and choices that can influence how they use technologies in the workplace.

For a discussion of Teleperformance’s webcam monitoring system, see Solon (2021). Teleperformance is a global call center company that provides both outsourced and U.S.-based call support for many major U.S. companies and specializes in “work-at-home” programs (see Teleperformance, 2018). See Doellgast and O’Brady (2020) regarding worker stress resulting from intense call monitoring practices.


See Luca, Kleinberg, Mullainathan (2016) and Frankowski (2019) for a discussion about the role of humans in shaping the objectives and design of algorithmic systems.

See Cappelli (2020) regarding management strategies and choices that can influence how they use technologies in the workplace.


See Luca, Kleinberg, Mullainathan (2016) and Frankowski (2019) for a discussion about the role of humans in shaping the objectives and design of algorithmic systems.

See Cappelli (2020) regarding management strategies and choices that can influence how they use technologies in the workplace.

For a discussion of Teleperformance’s webcam monitoring system, see Solon (2021). Teleperformance is a global call center company that provides both outsourced and U.S.-based call support for many major U.S. companies and specializes in “work-at-home” programs (see Teleperformance, 2018). See Doellgast and O’Brady (2020) regarding worker stress resulting from intense call monitoring practices.


For an overview of labor management systems and productivity monitoring in the warehouse industry, see McCrea (2020) and Dzieza (2020). See Vincent (2019) for more information about gamification in warehouses and Lecher (2019) regarding automated firing.

Gutelius and Theodore (2019) provide a comprehensive overview of technological change in the warehouse industry and Overstreet (2019) provides a brief overview of warehouse robots and order picking technologies. For a detailed overview of a lead-me cart task direction system, see Six River (https://6river.com/directed-picking/) and for a description of a voice-picking system, see Lucas (https://www.lucasware.com/voice-picking-introduction/).

For more information on EVV, see Cunningham (2019) and Metcalf (2018).

See Ticona, Mateescu, and Rosenblat (2018) for an overview of home care platforms. A growing body of research points to customer ratings as a source of bias, which, when used to inform management decisions or automate decisions about workers on platforms, can serve as a significant source of discrimination. See Rosenblat et al. (2016) and Dzieza (2015) for a discussion of customer ratings.

For overviews of technological change in the retail and grocery industries, see Carré et al. (2020) and Benner et al. (2020).


O’Connor (2016) describes the worker performance features of Percolata’s scheduling system. Also, see Tanaka et al. (2016) for a full description of the Percolata scheduling system in their patent application. Percolata has since incorporated surveillance cameras and computer vision into their system to measure in-store shopping traffic; see https://www.percolata.com/. For more information on the effects of scheduling optimization systems, see Kantor (2014) and Gleason and Lambert (2014).

Bhuiyan (2020) details Instacart’s system of performance metrics.

For more on algorithmically facilitated pay inequities at Shipt, see Lyons (2020).


For an overview of technological changes in the security industry, see Lasky (2019) and Mahmood (2019). See Knight (2021) and Lazzaro (2021) regarding errors in computer vision systems and Lever (2017) regarding privacy concerns with these systems. For examples of some of these systems, see Guardso (https://www.guardso.com/guard-tour-system?tab=reporting) and Silvertac Software (https://www.silvertacsoftware.com/automated-security-guard-management).

Peterson (2019) describes sensors and driver monitoring and scoring systems. See Clinton (2019) for an overview of recent technological developments in dash cam driver monitoring systems. Many of the same sensor monitoring technologies are also used to enable self-driving trucks; see Viscelli (2018). Also, see Levy (2015) for an analysis of the use of monitoring systems to exert control over truck drivers.
See Ticona, Mateescu, and Rosenblat (2018) for an overview of transportation network platforms, and Rosenblat (2016) and Scheiber (2017) for a description of how these companies use algorithms to manage workers.

For an overview of tabletop tablets, see O’Connor (2019). See O’Donovan (2018) and Rainey (2018) for information about servers’ experiences with these systems.

Matsakis (2019) describes the Presto restaurant monitoring system. See Knight (2021) and Lazzaro (2021) regarding bias and errors in computer vision systems.

See Eidelson (2017) and Jacobs (2018) for information on the history and status of panic button legislation and collective bargaining. See Lindzon (2020) for a discussion on the privacy and security risks posed by panic button systems and the variation in policies designed to protect workers.

For an overview of hotel service optimization systems, see Hotel Tech Report (2021). Escobar (2020) describes how many hotel technology vendors have adapted their systems to increase the ability for employers to monitor and scrutinize workers’ compliance with cleaning protocols in the context of COVID-19. Reyes (2018) describes the effects of these systems on workers.

For an overview of healthcare industry, see Litwin (2020).


See Harris (2017) and Maria and Burger (2016) for an overview of these systems along with some examples.

For examples, see Oliver (2020) and Woyke (2018).

See Condon (2019), State of Ohio (2018), and Chaney (2020) for information about automated benefit application systems.

For more information on automated decision-making systems in the public sector, see Chouldechova et al. (2018), Eubanks (2018), and Hurley (2019).

See Maurer (2021b) and Patton (2021).

For examples of new applications of workplace technology for COVID-19, see Negrón (forthcoming), Nguyen (2020), Rodriguez and Windwehr (2020), and UC Berkeley Labor Center (2020).

See Barocas and Selbst (2016) for a discussion about how data-driven systems can have a disparate impact. Ajunwa (2020), Bogen and Rieke (2018), and Kim (2017) describe bias in hiring algorithms and how they can result in discrimination.

See Jabsky and Obernauer (2019) and Ockenfels-Martinez and Boparai (2021) for documentation of health impacts at Amazon warehouses.

For example, research conducted by Doellgast and O’Brady (2020) found that intensive electronic monitoring in call centers was associated with higher levels of stress among workers.

For evidence on the link between job-related stress and health outcomes, see Nieuwenhuijsen, Bruinvels, and Frings-Dresen (2010).

For example, see Ikeler (2016) and Levy and Barocas (2018) for a discussion of the use of clienteling software in the retail industry to deskill sales jobs.

See TuSimple (2019) and Plus (2021) for a description of how truck drivers train algorithms designed to enable self-driving trucks and Sandu (2019) for a discussion on using call monitoring data collected from call center workers to train chatbots.
For a broader treatment of the effects of technological change on employment and wages, see Acemoglu and Restrepo (2019).

For example, see Tippett, Alexander, and Eigen (2017) regarding how scheduling software can enable wage theft.

See Gonzales (2016) and Townsend (2020).

For an overview of “fissuring” or business models based on outsourcing and contracting, see Weil (2019). See Rogers (2020) for some examples of fissuring and a description of the legal context that encourages fissuring.

Berfield (2015) describes social media monitoring practices used by a union avoidance consultant for Walmart.


For a discussion of the legal implications of electronic monitoring for labor organizing, see Garden (2018).

For example, Madden et al. (2017) describe how data-driven systems can harm low-income communities, including how social media data mining can exclude low-income groups from employment.

See Ajunwa (2018) and De Stefano and Taes (2021).

For example, see Hanley and Hubbard (2020) and Milner and Traub (2021).

See Lopez (2011) for a description of Disneyland’s use of leaderboards to motivate workers and Brodkin (2019) regarding a similar system used by Amazon.


For an overview of active state consumer privacy bills, see Klosowski (2021).

For legal analysis of the current gaps in protecting workers from data-driven technologies, see Ajunwa et al. (2017), Bales and Stone (2020), Barocas and Selbst (2016), Bodie (2021), Hirsh (2020), Kim (2017), Richardson (forthcoming), Rogers (2020), and Scherer and Brown (2021).

For example, see Wachter and Mittlestadt (2019).

For more detail on the patchwork of state privacy protections, see Ajunwa et al. (2017).

For a discussion on the difficulty of addressing discrimination and privacy issues created by workplace technologies, see Bodie and Kim (2021).

See Scherer and Brown (2021) for a detailed analysis of worker health and safety impacts from monitoring systems.

See Gamble (2019) and Milner and Traub (2021) for a discussion of the asymmetry of power these systems present for workers.

See Pasquale (2021) for a more general discussion about the limits of a consent model vis a vis digital technologies.


For a more general questioning of the privacy framework, see Morozov (2021). Also, see Tisné (2020) regarding the limitations of using an individual data privacy framework for regulating the collective harms that arise from data-driven systems.
Biometric data in particular will require heightened protections; see Ajunwa, Crawford, and Ford (2016) for a detailed analysis.

See Bottomley (2020) for examples of the data minimization principle in public policy.

For a detailed analysis of the connection between productivity monitoring and health and safety outcomes in the context of warehousing, see Ockenfels-Martinez and Boparai (2021).

A growing number of jurisdictions in the United States have placed bans on the use of facial recognition technology, particularly in the public sector. See Conger et al. (2019) and Simonite (2020).

Researchers have documented significant race and gender disparities and inaccuracies in the use of facial recognition technology; see Buolamwini and Gebru (2018) and Raji et al. (2020).

See Narayanan (2019).


Many of the concepts here are adapted from principles published by The Leadership Conference on Civil and Human Rights (2020). The authors also thank Professor Pauline Kim of Washington University in St. Louis for her generosity in sharing her expertise on discrimination law for this section.

See Bodie et al. (2017) and Rogers (2020) for a legal discussion on collective bargaining in relation to workplace data and technology decisions.

See Moss et al. (2021) and Reisman et al. (2018) for a framework on algorithmic impact assessments, geared towards the public sector. In the EU, algorithmic impact assessments have been legislated in the form of Data Protection Impact Assessments (DPIAs) under the General Data Protection Regulation (GDPR); see legal analysis from Kaminski and Malgieri (2021).

For a deeper study and analysis of algorithmic accountability in the public sector, see Ada Lovelace Institute (2021).
References


The Center for Labor Research and Education (Labor Center) is a public service project of the UC Berkeley Institute for Research on Labor and Employment that links academic resources with working people. Since 1964, the Labor Center has produced research, trainings, and curricula that deepen understanding of employment conditions and develop diverse new generations of leaders.

Suggested Citation


The analyses, interpretations, conclusions, and views expressed in this report are those of the authors and do not necessarily represent the UC Berkeley Center for Labor Research and Education, UC Berkeley Institute for Research on Labor and Employment, the Regents of the University of California, or collaborating organizations or funders.
June 29, 2023

Office of Science and Technology Policy  
Executive Office of the President  
Eisenhower Executive Office Building  
1650 Pennsylvania Avenue  
Washington, DC 20504

Submitted electronically via the Federal eRulemaking Portal at Regulations.gov.

Response to the White House Office of Science and Technology Policy Request for Information on Automated Worker Surveillance and Management

The UC Berkeley Labor Center welcomes the opportunity to provide input to the White House Office of Science and Technology Policy (OSTP) in response to the Request for Information on Automated Worker Surveillance and Management posted on May 1, 2023.

The mission of the Labor Center’s Technology and Work Program is to provide worker organizations and policymakers the research and policy analysis they need to respond to rapid technological changes in the workplace and ensure that technology benefits rather than harms workers. We focus on low-wage industries and the workers of color, women, and immigrants who are often on the frontlines of experimentation with emerging technologies.

We are very pleased to see the White House Office of Science and Technology Policy’s attention to automated workplace surveillance and management technologies and interest in exploring opportunities for Federal agencies to ensure that these systems do not harm workers and undermine their rights and opportunities.

Drawing from our own research analyzing trends in the data-driven workplace and impact of these technologies on workers, our goal in this comment is to highlight evidence indicating the prevalence of automated workplace surveillance and management technologies (Section I), impact on workers resulting from employers’ use of these systems (Section II), and principles and policy models for worker technology rights and protections (Section III). As an addendum,
we submit a few of our research publications which analyze trends in the data-driven workplace and provide a comprehensive framework of the technology rights that workers need and deserve.

Section I: Prevalence of automated worker surveillance and management systems

4. a. What data and evidence exist on the prevalence of automated worker surveillance and management systems across different industries, occupations, and regions, including changes over time?

There is a dearth of comprehensive, reliable data on employer adoption workplace technologies in the US. In fact, until the US Census Bureau first introduced questions about technology adoption in the Annual Business Survey (ABS) in 2018, the US government did not collect firm-level data on use of advanced digital technologies (e.g., AI) or robotics.¹ But, unfortunately, the 2018 ABS survey did not directly ask questions about automated worker surveillance and management systems.

Nevertheless, the 2018 ABS does provide nationally representative survey data of private, non-farm firms in the economy on the diffusion of advanced technologies, including: artificial intelligence (AI), cloud computing, robotics, and the digitization of business information. According to an analysis of the survey data conducted by the Center for Economic Studies, 6.6% of firms used some form of advanced “AI-related” technology in the workplace in 2018. Although the share of firms adopting advanced technologies is relatively low, worker exposure is higher because the firms adopting these technologies are some of the largest companies in the US. Firms that have adopted at least one type of advanced business technology employ more than 40% of all workers, and firms that have digitized at least one form of information and have invested in cloud services – the building blocks of more advanced technologies – employ more than 90% of all workers. That said, it remains unclear the extent to which each of those workers was directly exposed to all technologies adopted by the firm.

The 2019 ABS incorporated questions focused on workforce impacts of artificial intelligence, cloud services, specialized software, robotics, and specialized equipment with an emphasis on worker displacement.² Once again the survey did not directly inquire about the use of workplace technologies to monitor and manage workers. Analysis of the survey data indicates that 40% of firms, employing 64% of US workers, use some type of specialized software. Although the ABS surveys do not provide a direct measure of the prevalence of worker electronic monitoring and automated management technologies, they do give a general indication of employer adoption of digital technologies that can provide a foundation for more advanced data-driven workplace technologies. Moreover, many of the software technologies used to produce goods and services also enable employers to monitor worker activities and behaviors. For further reference, we outline these studies and other privately commissioned studies in a recent working paper.³
Another strategy for exploring employer adoption of electronic monitoring and automated management technologies is to collect data from workers. Kristen Harknett and Daniel Schneider with the Shift Project recently conducted a survey of workers on the prevalence of worker surveillance and automation in the retail industry. Using a Facebook ad sampling approach, they surveyed 10,000 retail and food service workers employed by 140 different US employers in Fall 2022. Initial findings presented at a recent UCSF California Labor Lab conference indicate that 80% of workers reported their employers use technology to monitor the quality of their work, and nearly 25% workers reported that it was at least somewhat likely that their employers were monitoring them outside of work. Given that the retail industry is one of the largest employers in the US, this research provides a glimpse into the extent of employer adoption of workplace electronic monitoring technologies.

Despite the lack of comprehensive and representative data on employer adoption of electronic monitoring and automated management technologies, a growing body of evidence suggests that employers are using these technologies across a wide range of industries. Research and media coverage feature numerous examples of firms using data-driven technologies to electronically monitor and manage workers across industries in the economy. Moreover, the landscape of vendors offering technologies to monitor and manage workers has exploded over the past few years. For example, a recent engineering article reviewed 89 commercial workplace wearable applications designed to monitor workers across a wide range of industries for a variety of purposes including health, productivity, and safety. Wearables are just one segment of the workplace technology product market focused on monitoring and managing workers. In a 2021 study, Coworker.org identified 550 vendor products on the market offering systems for employers to monitor and manage workers. Meanwhile, venture capital and private equity investors have funneled over $15 billion in HR technology start-ups in the last few years. Although not all of the HR technologies are designed to directly monitor and manage workers, “employee listening” and performance management systems are a growing segment of the market and are increasingly incorporated into standard HR technology platforms.

Overall, based on the available evidence, it is clear that technology development trends continue to afford employers with the capability to electronically monitor and automate worker management, and some employers are currently deploying those systems in the workplace. Incorporating questions about employer use of technologies for electronic monitoring and management in future government surveys, such as the US Census Bureau Annual Business Survey (ABS), as well as other agency surveys conducted by the Federal government, will be crucial to help us provide a better understanding and documentation of employer technology adoption and use, and the impacts of these technologies on workers.
Section II: Impacts on workers resulting from employers' use of these systems

4. b. What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers’ pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

Employer use of electronic monitoring and automated management systems can have profound consequences for wages, working conditions, race and gender equity, and worker power. In a 2021 UC Berkeley Labor Center report, *Data and Algorithms at Work: The Case for Worker Technology Rights*, we outline examples of potential harms that can result from workplace electronic monitoring and automated management technologies in a wide range of industries. These harms include discrimination, work intensification and speed-up, hazardous working conditions, deskilling and automation, growth in contingent work, loss of autonomy and privacy, and suppression of the right to organize.

In a subsequent UC Berkeley Labor Center report published in 2022, *Technological change in five industries: Threats to jobs, wages, and working conditions*, we synthesize findings from five industry studies conducted by experts in trucking, warehousing and logistics, health care, retail, and food delivery. In each industry studied, researchers found that although there are examples of employers' use of new technologies in ways that are helpful to workers, many employers are prone to use new technologies in ways that threaten working conditions, wages, and job quality. Of particular concern is that employer experimentation with new technologies in the front-line industries studied can worsen existing labor market inequities for workers of color, women, and immigrants who are overrepresented in the occupations in those industries. However, as outlined in the report, the outcomes of employer adoption of emerging technologies is not predetermined. The social and institutional context shapes employer decision-making about new technologies, leading to variation in adoption and worker impacts.

Finally, in a 2023 UC Berkeley Labor Center blog post, *35 Years Under Electronic Monitoring and Still Waiting for Worker Rights*, we highlight findings from decades of research linking electronic performance monitoring (EPM) with worker stress and other harms. According to a comprehensive meta-analysis of 94 research studies conducted in 2022, EPM systems increase stress for workers, regardless of the monitoring systems’ specific characteristics. The studies included in the analysis focused on a range of stress indicators from psychological strains to physiological conditions, with all studies finding consistent EPM effects on worker stress. Workers can experience stress as a direct result of the fact and knowledge of being closely monitored, but the impacts of EPM systems on working conditions, job/task design, and work environment can also indirectly increase stress for workers. Importantly, the 2022 meta-analysis study found “little evidence” that electronic performance monitoring systems actually increase worker performance.
4. c. What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers' abilities to form and join unions and bargain collectively with their employers?

At this point, most of the evidence available documenting the impact of workplace monitoring and automated management technologies on labor rights is mainly information about the systems available on the market and their capabilities, not yet on the actual impact on workers' abilities to form and join unions and bargain collectively with employers. However, we do have evidence that emerging technologies have enabled a variety of employer practices that threaten workers' rights to organize and form unions. Data-driven systems enable employers to profile workers and make predictions about their propensity to organize or join unions, to predict the risk of potential unionization within a company as part of a strategy to prevent organizing efforts, and to map and track organizing and unionization drives to target and tailor union avoidance campaigns.

As a pre-employment strategy, many vendors offer social media monitoring products to screen out job candidates who might raise concerns about the company. For instance, FAMA, a technology vendor specializing in data mining job candidates' personal social media accounts, offers a product designed to identify potential " whistleblowers, scammers, and violent insiders" likely to engage in "toxic" or "risky" behaviors that might threaten the reputation of the employer. Similarly, Social Intelligence, another social media screening company which was acquired by FAMA in 2023, allows clients to develop custom filters with keywords to identify activist job candidates that pose a risk to the company. Employers and vendors also use personality assessments and data analytics to predict the likelihood of union sympathies among job candidates. Although these pre-employment vendors do not explicitly state they are trying to identify pro-union candidates, which is an unfair labor practice under the NLRA, personality tests and social media screening can obscure these intentions making a case difficult to prove. In fact, a key feature of data-driven technologies is the ability to generate data proxies for information that is protected or unavailable by data mining public data sources and making predictions about unknown characteristics or traits. The union avoidance industry is aware of this ambiguity and suggests working with technology vendors to help screen in workers who have characteristics unlikely to be open to unions.

Social media data mining technologies also enable employers (and third-party vendors and consultants) to monitor current employees' social media for potential organizing efforts and during collective organizing campaigns, such as union elections and strikes. For example, HelloFresh used Falcon (now Brandwatch), a web crawling and sentiment analysis system, to mine Twitter and Instagram for employee posts about unionization efforts and workplace concerns. McDonald's took their social media monitoring efforts one step further by conducting social network analysis by creating fake Facebook profiles to track labor organizers involved in the Fight for 15 campaign and identify workers involved in the movement and their networks. Even more disconcerting is that military and corporate intelligence firms are deploying passive data collection and open-source intelligence gathering strategies to help employers identify and
map social organizing networks and monitor organizers and union campaigns. For instance, vendors originally designed for monitoring global security threats by mapping terrorist social networks are branding their products for corporations to use for “insider threat assessment” including unionization drives. Likewise, Walmart contracted with Lockheed Martin to monitor worker organizers’ social media activity. As reported in Bloomberg, Lockheed Martin used their proprietary data analytics system, LM Wisdom, described on their website as a “tool that monitors and analyzes rapidly changing open-source intelligence data … [that] has the power to incite organized movements, riots and sway political outcomes.”

In addition to social media monitoring network analysis, vendors and employers also use “employee engagement” surveys and algorithmic systems to predict unionization risks. For example, IRI Consultants, a union avoidance consulting firm, recommends using data analytics services to predict employee likelihood of voting for a union in an organizing campaign. IRI highlights Perceptyx, an “employee listening” and “employee engagement” vendor that offers a “union vulnerability index” product designed to predict risk of unionization. Perceptyx’s predictive model draws from millions of historic survey responses across employers to build profiles of employees vulnerable to unionization. To assess employee vulnerability, the company combines passive data collection (messages on systems like Slack and Microsoft Teams, email messages, and calendar events) with active data collection (engagement surveys) to make predictions about at-risk employees who might support unionization efforts.

According to IRI, employers can use these predictions to preempt potential union activity among employees with a union avoidance campaign. Recent media coverage on the union avoidance efforts of Amazon, Whole Foods, and other companies across industries illustrate how employers can use risk scores to target resources to the specific workplace locations. Amazon and Whole Foods developed a predictive model based on data collected through employee surveys, “tipline” calls, employee demographics and metrics, health and safety records and OSHA violations, and local labor union context to generate “heat maps” marking which stores are likely to unionize.

Although many of these technologies are simply new manifestations of old strategies, they enable employers unprecedented abilities to surveil workers in and outside of work. As these examples suggest, many vendors, consultants, and employers know they can shield their union avoidance strategies from scrutiny with the novelty and opacity of these technological systems. At a time of extraordinary worker organizing and push for unionization over the past few years, these examples illustrate how emerging worker surveillance and management technologies empower employers to suppress workers’ labor rights.
Section III: Principles and policy models for worker technology rights and protections

5. b. Are there policy approaches to regulating automated worker surveillance and management systems from state, Tribal, territorial, or local governments or other countries that Federal agencies could learn from?

For the majority of US workers who are not union members, the profound asymmetry of power in the workplace means they have little to no say over the policies and decisions that affect them in their day-to-day work lives. In particular, notions of consent to new technologies or the ability to find better conditions elsewhere are not meaningful or available to low-wage workers, women, and workers of color, who face a labor market that is often dominated by employers competing by cutting labor costs. US employment and labor laws have long attempted to balance this asymmetry of power in the employment relationship by instituting labor standards and policies, and giving workers a mechanism for exercising collective voice. Those laws and policies now need to be strengthened and updated for the 21st century workplace and its technologies.

For example, we are pleased to see recent developments across federal agencies, such as the NLRB General Counsel’s 2022 memorandum on increasing enforcement of worker surveillance that interferes with workers’ rights to organize, as well as the Equal Employment Opportunity Commission’s (EEOC) recent Title VII guidance for employers to prevent the use of algorithmic systems from leading to discrimination in the workplace. Both are important steps to protecting workers’ labor and civil rights. Continued guidance for employers and vendors combined with rigorous enforcement of violations along with health and safety, wage and hour standards will help bolster worker protections in the face of emerging technologies.

We believe that the US needs a new set of 21st century labor standards establishing worker rights and employer responsibilities for the data-driven workplace. These standards should be established both in public policy and in collective bargaining agreements in unionized workplaces. In our report, *Data and Algorithms at Work: The Case for Worker Technology Rights*, we outline a comprehensive set of policy principles that can help build a robust regulation regime. The principles lay out a vision for labor standards that (1) give workers rights with respect to their data, (2) hold employers responsible for harms caused by their technology systems, (3) regulate the ways in which employers monitor workers, use algorithms, and make decisions based on those systems, (4) require impact assessments that test for a broad range of harms to workers, (5) ensure the right to organize around technology, (6) guard against discrimination, and (7) establish a strong regime of worker recourse and public enforcement.

The comprehensive framework laid out in our report has not yet been adopted in the US. Regulation of automated worker surveillance and management systems is currently limited, but there are growing efforts by policymakers and advocates at the federal, state and local level to address the impacts of these systems. Recently state legislators have introduced the Workplace
Technology Accountability Act (AB1651) in California and An Act Preventing a Dystopian Work Environment (H1873) in Massachusetts, two bills that in our analysis are currently the strongest worker technology rights proposals in the US. Both have been informed and supported by unions and other worker advocates on the frontlines of technology implementation, and both embrace the policy standards of transparency, responsible use, and accountability detailed below (the Massachusetts bill was drafted as a version of the California bill):

1. Transparency

- **Full disclosure**: Employers should provide workers with clear notice of any data-driven technologies used. Notice of electronic monitoring should include a description of which activities will be monitored, the method of monitoring, the data that will be gathered, the times and places where the monitoring will occur, and the purpose for monitoring and why it is necessary. Notice of algorithm use should include an accessible description of the algorithm, its purpose, the data it draws on, the type of outputs it generates, and how the employer will use those outputs in their decision making.
- **Explanation**: Employers should provide an explanation of how their use of data-driven technologies such as electronic monitoring or algorithmic decision-making can affect employment decisions, including their assessment of workers’ performance or productivity.
- **Data protection**: Workers should have the right to access, correct and download their data. Employers should minimize the use of workers data to only when it is necessary and essential to workers doing their job.

2. Responsible Use

- **Limits on electronic monitoring**: Employers should minimize the use of electronic monitoring for narrow purposes that do not harm workers and respect workers privacy. Employers should not monitor workers when off duty. Electronic monitoring should not be used as a substitute for human decision making nor automate decisions around hiring, firing, discipline and promotion.
- **Limits on algorithmic management**: Employers should not use algorithms that harm workers’ health, safety, and wellbeing. Employers should not use algorithms to make irrelevant or unfair predictions about workers that are unrelated to their job responsibilities, including predictions about their emotions, personality or health. Algorithms should not be used as a substitute for human decision making nor automate decisions around hiring, firing, discipline and promotion.
- **Limits on high-risk technologies**: Employers should not use unproven or high risk technologies like facial recognition.

3. Accountability

- **Thorough impact assessments**: Impact assessments should be made before use of algorithms or data collection and reviewed by the relevant regulatory agencies. Technologies should be continuously evaluated and harms mitigated. Workers should
have a role in these assessments and be able to challenge them. Risk evaluations must include the risks of discrimination against protected classes, if such risks are found, the assessments must be shared with the state agency overseeing workplace discrimination.

- **Robust enforcement:** Regulatory agencies should be able to respond to worker complaints, apply penalties, initiate investigations and pro-actively audit technology use. Workers should also have the private right of action to enforce their rights.

The California (AB1651) and Massachusetts (H1873) bills are important models for regulation based on the principles of transparency, responsible use and accountability and because they recognize the importance of full disclosure and transparency as a foundational right. However, importantly, these policies move beyond the notice and consent framework underlying many data protection policies by establishing protective guardrails on employer collection of worker data through electronic monitoring and use of high-risk technologies, such as facial or emotion recognition technologies, that pose significant harms to workers. Importantly, these policies cover all types of workers, including W-2 employees and independent contractors, which is key to ensuring all workers are covered by the law.

Additionally, these policies include robust enforcement measures including a private right of action for workers to pursue claims against the employer and the authority for the labor agency to investigate, apply penalties, conduct audits, and obtain injunctive relief, shifting the burden away from workers to seek redress for harms and onto employers to ensure the technologies they deploy do not harm workers.

The right to organize and bargain is a key aspect of worker technology rights that goes beyond the California and Massachusetts bills. Recognizing that the major challenge to fair and equitable workplaces is the deep imbalance of power between employers and workers, policies that protect workers well-being and their ability to meaningfully consent and have agency around new technologies that impact them should include upholding the right to organize and bargain. Workers need the right to collectively organize and have a say around workplace technology and its impacts on them, and when represented by a union, to bargain collectively around it. Employers should not use technologies to identify, monitor, or punish workers for organizing.

While not nearly as extensive as the two bills described above, the 2018 California Consumer Privacy Act (CCPA) and the subsequent California Privacy Rights Act (CPRA) – amendments introduced through a 2020 referendum to strengthen the law – is an example of a first step towards worker data rights that has actually passed into law. As of January 1, 2023 the CCPA/CPRA provides all workers, including independent contractors, with the right to be notified when employers are surveilling them, and for what purpose. They have the right to access their data, and ask to correct or delete it. And they will be able to opt-out of employers selling their data.
The other noteworthy law that provides workplace protections with respect to electronic monitoring and automated management technologies is the Warehouse Distribution Centers Law (AB 701), which sets guardrails around warehouse quotas in California. Currently, legislators in other states have introduced similar bills in Connecticut (CB 152), Minnesota (HF 2774), New York (SB 8922), and Washington (SB 5891)).

Ultimately, we believe that workers should fully participate in decisions over which technologies are developed, how they are used in the workplace, and how the resulting productivity gains are shared. This participation need not and should not be anti-innovation, because workers have a wealth of knowledge and experience to bring to the table. Dehumanization and automation are not the only path. With strong worker protections in place, new technology can be put in the service of creating a vibrant and productive economy built on living wage jobs, safe workplaces, and race and gender equity.

Thank you for the opportunity to provide these comments.

Annette Bernhardt, PhD  
Lisa Kresge  
Kung Feng 
Director  
Lead Researcher  
Policy Researcher 
Technology & Work Program  
Technology & Work Program  
Technology & Work Program

Attachments:
Full Comment: UC Berkeley Labor Center Response on Automated Worker Surveillance and Management
Report: Technological change in five industries: Threats to jobs, wages, and working conditions

Endnotes


Perceptyx https://www.perceptyx.com/;


At the federal level, see the recently introduced the Stop Spying Bosses Act (S 262) and Algorithmic Accountability Act of 2022 (HR 6580).

PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0189
Comment on FR Doc # 2023 12995

Submitter Information

Name: Lilly Irani
Address:
Email:
Phone:

General Comment

Please accept this edited summary and working paper detailing Amazon's automated surveillance and management techniques on the Amazon Mechanical Turk platform. For questions, please email Lilly Irani, Associate Professor UC San Diego, Faculty Director UC San Diego Labor Center at

Attachments

Irani Algorithms of Suspicion Working Paper - 6
When Managers Rely on Algorithms of Suspicion: Fraud Logics and Their Fallouts

LILY IRANI
July 4, 2022
Two decades ago, platform champions promised that digital platforms would enable transparency and ease access to media, work and government services. In attempting to broker these relationships at scale, platforms have created the problem of vetting large volumes of unknown participants while minimizing their investments in human workers to mediate participant-platform relationships. Managers of these platforms adopt a philosophy of automated management, where opaque machine-learning algorithms designed for fraud detection are used to guess the “bad actors.” Companies use these algorithms of suspicion to dispense with workers based on risk in the name of fraud. The law lets them.

Workers for whom jobs might be a lifeline could wake up one day to find themselves cut off from work without notice. For those brave or stubborn enough to contest it, they may be met by silence from platform technical support. They may be told that there is nothing the platform can do. Or, if they are lucky, the platform may investigate their case and determine their account was suspended in error. In those cases of repair, companies do not redress their error by restoring lost earnings.

Innocent activities such as sharing infrastructure can be flagged as fraud when algorithms are trained to assume each user has a different Wi-Fi network. For example, a data-processing worker in the United States woke up one morning and found herself locked out of her job. On a normal day, she did data processing, transcription and classification — the type of work that powers much of the internet and artificial intelligence. That day, however, she found herself locked out of the marketplace where employers were offering the day’s work. Only after the worker-run advocacy group Turkopticon\(^1\) intervened did Amazon reinvestigate the suspension and admit it had made a mistake. The worker’s account had been suspended because she and her son had logged in from the same Wi-Fi router at home and, thus, had the same Internet Protocol (IP) address. Amazon had interpreted the second login on the same IP address as a worker trying to get paid to do the same social science study twice with different accounts, corrupting research results. Algorithmically accused of fraud, she had no legal right to recourse in her legal jurisdiction, despite there being no prohibition on working from the same place in Amazon’s terms of service. Amazon investigated and explained that it made an error; however, it offered no compensation for the two weeks of income that the data-processing worker had lost.

While Amazon uses fraud algorithms to guess at bad actors, it uses other algorithms to elevate some workers as trusted. Amazon’s Mechanical Turk platform has developed a program it calls “Masters.” Amazon promotes Masters workers as trusted producers of high-quality work on the platform, a premium for workers. Masters workers get exclusive access to a large stream of work; however, Amazon takes a larger cut of what other employers pay.

Workers express frustration and confusion about how to gain access to Masters work. Workers with very high ratings or long track records may not receive the designation. Masters acts as a kind of algorithmic glass ceiling installed by Amazon. A 2014 Amazon patent\(^2\) holds some clues as to how Amazon grants workers this privileged status. The patent suggests that Amazon may calculate a “judge error rate” or confidence rating it assigns to workers behind the scenes\(^3\). The patent also suggests that Amazon has several strategies for judging the quality of workers. It might place hidden tests with known answers to test individual workers. More controversially, it may have multiple workers complete the same work task but — not knowing the answer to the task — it will judge the workers who give the most popular or “plural” answers correct. This way of measuring correctness judges workers as less competent when their interpretations deviate from the norm, even if the question is subjective.

The automation of trust and suspicion can justify unintuitive and expansive forms of corporate surveillance in search of signals of risk.

More disturbingly, the Amazon patent also suggests that workers may be evaluated by the speed of task performance, alongside accuracy and error rate. The patent authors, perhaps, do not imagine users with disabilities — for example, repetitive stress injury, impaired vision or neurodiverse cognition — as good workers. Workers who are slower because they are juggling care work in the home may also be judged as less competent in their approach. At the scale of data work Amazon processes, the patents evidence an approach that seeks to automate at the cost of indifference to situations shaped by gender or disability.

The automation of trust and suspicion can justify unintuitive and expansive forms of corporate surveillance in search of signals of risk. One patent titled “Authentication and fraud detection based on user behavior”\(^4\) describes a technique to
These machine-learning approaches do not make rules about what makes a good or bad worker that can easily be explained. Rather, they describe signals that machine learning will “learn” to hone in on as it infers a way of guessing which workers are “good” or “bad.” Workers then can be flagged for seeming close to workers — in the eyes of the algorithm — who were previously judged as bad, or seeming far from workers who were judged as good. To be an outlier, rather than breaking a rule, can be enough for the company to flag a worker as a problem.

Fraud engineers who build models often recognize that the algorithms make imperfect guesses, and might recommend, as Anne Jonas and Jenna Burrell (2019) found, that companies use the algorithms to launch an investigation, engage with the user and then decide how to act.

Amazon, like many companies, seems to jump straight to punishing flagged accounts without a clearly outlined appeal or redressal process. Former Amazon engineers, Spencer Soper (2021) reported, told management that innocent people might be flagged as bad actors, but management chose to suspend first, correct later (and only for those workers who pursued the matter). Managerial departure from engineering recommendations is not surprising, as companies place all the costs of algorithmic mistakes on the shoulders of workers.

Emerging digital rights frameworks have loopholes that leave workers accused of “fraud” without transparency or recourse. California’s marketplace rights law (AB 1790) requires marketplace operators to disclose grounds for suspending a marketplace seller, except if it could “negatively impact the safety or property of another user or the marketplace itself.” The California Consumer Privacy Act (CCPA) of 2018 also exempted companies from deleting consumer data on request if data would be kept to “detect...fraudulent...activity, or prosecute those responsible for that activity.” (A 2020 voter initiative amended this exception in the CCPA.) Companies argue that revealing their algorithms only empowers “adversaries” seeking to game the system.

Companies protected by this opacity shoot first and apologize later, if at all. The law provides little disincentive to tech company commitments to large-scale workforces with largely automated industrial relations. This is not a problem of engineering knowledge but rather a problem of companies that treat workers as disposable and without the right to due process. Policy makers must look to workers on platforms, such as those of Turkopticon, who are experts in the kinds of harms and vulnerabilities they face and create policy that strengthens their voice in the platforms they power through their work.

Acknowledgment

Thank you to the worker organizers of Turkopticon for their insights and contributions to this work.

---

1 See www.blog.turkopticon.net
3 bid Figure 1

Works Cited

Jonas Anne and Jenna Burrell 2019 “Friction snake oil and weird countries Cybersecurity systems could deepen global inequality through regional blocking” Big Data & Society 6 (1) 1 11

Algorithms of Suspicion: Authentication and Distrust on the Amazon Mechanical Turk Platform

Dr. Lilly Irani, UC San Diego

Draft under review at MIT Press for publication in Global Platform Governance (Center for International Governance Innovation ed.)

Abstract

This chapter examines the assemblage of policies, practices, and algorithms of suspicion that control workers’ access to wages and work on digital labor platforms. I show how “fraud” acts as a quasi-legal category that legitimizes and protects platform operators’ unilateral decisions to fire workers. This case study begins with the problem of opaque account suspensions suffered by good faith workers on the platform Amazon Mechanical Turk. Through an investigation of patents, research papers, and industry documentation, the chapter constructs a view of the models and assumptions Amazon deploys to guess the difference between good and bad workers. These algorithms and the opaque organizational routines that deploy them submit workers to automated surveillance, suspicion, and terminating action – managing workers at scale and at a distance. These practices may have discriminatory consequences, sometimes in ways recognized by legally recognized protected categories and sometimes not. The chapter concludes by arguing that existing digital rights frameworks must be revised to give workers rights and protections against platforms’ algorithmic forms of management.

Introduction

Platform workers for whom jobs might be a lifeline could wake up one day to find themselves cut off from work without notice. The reasons might be a software glitch, a change of address, or myriad others as this chapter’s analysis will reveal. For those workers brave or stubborn enough to contest it, they may be met by silence from platform technical support. They may be told that there is nothing the platform can do. Or, if they are lucky, the platform may investigate their case and determine their account was suspended in error. In those cases of repair, companies have not redressed their error by restoring earnings workers lost shut out of their accounts. Turkopticon, one platform worker advocacy project, assists many workers in this situation. The consequences are lost access to livelihood, already earned wages trapped in platform accounts, and a deep
sense of frustration and unfairness. Workers report such experiences of automated firing, wage theft, and platform silence on myriad gig work platforms, including Uber, Lyft, Doordash, and, the focus of this chapter, Amazon Mechanical Turk (AMT).

This chapter builds on scholarship on automated shop floor management – a problem that includes but is also broader than platforms. Jeremias Adams-Prassl has examined how the introduction of algorithms into employer functions of hiring, monitoring, and firing concentrate managerial control over work while also making responsibility and accountability difficult to track. Nantina Vgontzas explains how algorithms in Amazon’s warehouse operations are central to controlling workers. They do this through surveillance and control of rates that produced gendered and racialized hierarchies in the workplace. The algorithms, engineered by Amazon’s own tech workers, also direct packing and shipping to work around sites of work slowdowns or strikes, making it more difficult for workers to engage in effective, concerted collective action. More broadly, a wide ranging scholarship on gig work has debated platforms’ forms of control through reputation systems, gamification, and debt, as well as platforms’ strategies of legal and especially employment (mis)classification.

This chapter contributes to these debates by drawing attention to a form of algorithmic control and wage theft through account suspensions on one such platform, Amazon Mechanical Turk. Policy gives platforms wide berth to suspend under laws that exempt “fraud detection” activities from oversight and transparency frameworks. In many jurisdictions, workers are also (mis)classified as independent contractors, lacking rights of recourse in cases of firing. Finally, Amazon’s algorithms – marketed to other companies as Amazon Fraud Detector – are also of consequence not only to its platform workers, but to small businesses and consumers on its wider website and to internet users at large. As goes Amazon, so goes the world?

This chapter draws as data the experiences and insights of AMT workers faced with the problem of account suspensions, analyses of how AMT’s interfaces and policies structure and automate employer-worker interactions, and analyses of patents that give clues as to Amazon’s black box fraud detection algorithms unleashed on workers at scale. I show legitimate reasons why workers might get caught up by Amazon’s algorithms that catch workers whose behavior appears suspicious to an algorithm with no social or political knowledge of their lives. The chapter
concludes by arguing that existing digital rights frameworks must be revised to give workers rights and protections against platforms’ algorithmic forms of management. I offer preliminary suggestions to this end.

This is a work of engaged scholarship, accountable to workers on the frontlines experiencing these workplace issues at the intersection of policies, practices, and algorithms. The research is particularly indebted to the work of AMT workers organizing as Turkopticon, a project that advocates for better working conditions for workers. An important part of their work is assisting AMT workers whose contesting account suspensions. Workers’ problems and insights motivate and inform this chapter’s inquiry. Workers’ comments on this paper and conversations have informed its development. This work is informed by methods such as Community-Based Participatory Research and Design Justice. From those methods, I adopt accountability to communities and a respect for communities’ expertise in many circumstances that affect their lives.

Policy, practices, and design are mutually constitutive in complex systems design. Workers encountering these problems propose solutions that might require shifts in one or more of these three aspects. Solutions to the problem of account suspensions likely requires changes in intermediary (e.g. platform, company, employer) practices, including algorithm design processes, how employers (e.g. platforms) employ algorithmic judgements, and how they prevent or repair unwarranted harm to workers from those judgements. Solutions may also require changes to the algorithms themselves, the data sets on which the algorithms are trained, or the ways in which outputs are applied. Finally, policy environments set the conditions in which companies configure these algorithmic processes, create risks for workers, and distribute the costs of those risks. This chapter analyzes AMT’s fraud practices as co-constituted by organizational practices, algorithms, and a permissive legal environment that allows algorithmic managers wide berth to opaquely regulate workers without worker redress.

**Amazon Mechanical Turk: Classifying cultural data for AI**

Amazon Mechanical Turk (AMT) is a data work marketplace that powers machine learning (ML) and artificial intelligence (AI) pipelines across the tech industry. Amazon launched AMT in 2006 to allow programmers to issue data processing calls directly from their computer code.
Rather than other code answering the call, thousands of workers wait at their computers, ready to perform cognitive piecework on demand. The system, and systems like it, are critical to the production of ML and AI.

AMT workers choose among tasks like transcription, content moderation, and image classification, getting paid per piece of data processed. They categorize and classify data so that machine learning algorithms can learn to approximate Turkers’ judgements. Sometimes the workers help train AI. Other times, they make up for AI’s shortcomings. A company that scans customer receipts into budget software, for example, would send the faded or irregular receipts that confused its algorithms to AMT workers to transcribe and enter into the software. AMT workers may also participate in social science experiments and data gathering as paid participants. AMT workers, in short, perform those tasks of cultural judgement they learn to perform through a lifetime of cognitive and cultural development.

Amazon first patented the system in 2007 to help organize products from different sellers on Amazon’s marketplace. Engineers faced a problem: they had data, including pictures and text, about products from different merchants to display on their websites. A stream of products uploaded by merchants, of, say, pens may not have a standardized identification number. For example, are products titled Lamy Safari, Lamy Safari Pen, Lamy Safari Fountain Pen, and Lamy Fountain Pen Cartridge the same product? Computers cannot tell without human interaction. A person familiar with fountain pens might easily say that the first three are names for the same thing but the last is a different object, even though each phrase differs from the next by only one word. So Amazon’s engineers had a problem. How could they automate the process of creating just one page for a product and linking to different merchants that offer the product but describe it in varying ways?

This kind of problem is one of organizing cultural data – data that contains cultural categories produced and changed by people as they interact through language and symbols. Artificial intelligence, machine learning, platform content moderation are all examples of attempts to automate at least part of the process of organizing, filtering, and responding to cultural data. The engineer’s goal is to extract correct categorizations from workers to train machine learning or substitute for it when it fails. Just as a lot of work goes into quantifying and scaling the messy
world so it can be represented statistically, a lot of work also goes into both producing correctly
classified data sets to produce these models, as well as correcting the answers of models when
they fail. Correct here is employers who enforce dominant culture definitions and conventions
through their task design and criteria.  

On Amazon Mechanical Turk, this work is completed by over 120,000 registered workers,
through only 30,000 were active in a given month according to one 2020 study. A 2016
International Labour Organization (ILO) study found that 45.2% of US and 90.7% of Indian
AMT workers had college or post-graduate degrees, belying assumptions that workers on the
platform lacked sufficient education to gain higher paying work. The ILO study found that
almost 85% of workers were based in the US, 15% were from India, and a small percentage were
from other countries. Workers, the ILO found, came to the platform for many reasons, including
to complement pay from other jobs, to combine work with child or elder care, and to earn a
living with a disability.  

**Recruiting 1,000 workers in a day**

Employers outsourcing data processing work to the AMT platform create batches of tasks, called
“human intelligence tasks” or “HITs” in Amazon parlance. HITs are web-based forms, hosted on
Amazon’s platform, that specify an information task and allow workers to input a response.
Tasks include structuring unstructured data (e.g. entering a given webpage into an employer’s
structured form fields), transcribing snippets of audio, and labeling an image (e.g. as
pornography, or violating given Terms of Service). Employers define the structure of the data
workers must input, create instructions, specify the pool of information that must be processed,
and set a price.

The employer then defines criteria that candidate workers must meet to work on the task. These
criteria include the worker’s “approval rating” (the percentage of tasks the worker has performed
that employers have approved and, by consequence, paid for), the worker’s self-reported country,
and whether the worker has completed certain skill-specific qualification exams offered on the
platform. This filter approach to choosing workers, as compared to more individualized
evaluation and selection, allows employers to request work from thousands of temporary
workers in a matter of hours.
One consequence of seeing people at scale has been that engineers imagine a world of “customers” and “bad actors.” In their public writings to one another, engineers worry about two kinds of “bad actors”: workers using scripts to generate random answers and hoping to get away with it, as well as workers not competent in the cultural categories needed by requesters. Workers might also produce “errors” because of interface design, exhaustion, undesirable interpretations, or simply by accident. AMT’s restrictive interface prevents employers from knowing the difference between good faith errors, good faith cultural mistranslation, and bad faith “spam” work in many cases.

The language of “bad actors” reflects a wider culture of security beyond Amazon Mechanical Turk. It is common for large computer system operators, from corporations to the military, to operate in an imaginative geography of “good” and “bad actors.” In such a world, engineers often see themselves in warfare with “bad actors” trying to “game the system.” The more “bad actors” know about how the system operates, the more they can game it – or so the “security by obscurity” story goes. Conversely, engineers charged with protecting systems use the data available to them to identify and block “bad actors” from accessing the system. In a world of platforms made into a cybersecurity battleground, collateral damage is common.

In 2018, the “bot scare” erupted in the world of Amazon Mechanical Turk workers and employers, illustrating how employers imagine mundane workplace challenges as threats by “bad actors” or quasi-criminals. The scare began when a graduate student posted to a Facebook group of other Amazon Mechanical Turk employers observing that he was seeing more surveys with nonsense answers and respondents with identical locations. By the end of the week, researchers all over the internet were reporting similar concerns, fearing that their published research papers had analyzed spurious data produced by automated scripts – automated scripts animated by workers defrauding well-meaning researchers and breaking Amazon’s terms and conditions along the way. Crowdsourcing research firm CloudResearch produced a study involving a range of tasks meant to discern whether answers were produced through automation or human input. They reported that odd results were not bots at all, but rather workers who performed well on certain questions and poorly on others. These workers, often in south Asia, performed worse on certain kinds of tasks not designed with their capabilities in mind, but actually performed better than US workers on tasks geared towards their cultural knowledge.
Requesters’ panic about fraudulent workers in fact masked their lack of awareness of who their workers were, what their skills were, and what tasks they might be suited to.

Patents and reported practices reveal a range of ways engineers attempt to discern “bad actors” from workers they ought to trust. They do this both at the scale of assessing work products, or HIT results, and also at the scale of assessing workers.

Assessing work products

Engineer-employers need to authenticate answers from untrusted workers to common data classification tasks that provide fuel (training sets, algorithmic evaluations) for machine learning. The engineer can extract answers from workers, but how can they know which answers are correct by their standards? Remember they are working with large volumes of data work output so they can’t review answers individually. And they are dealing with socially negotiated categories and meanings. Is this porn or not porn is only the most extreme example. I have not yet seen an engineer grapple with anthropological questions of whether multiple answers can be “correct” in different contexts.

Engineers have several ways of dealing with this uncertainty. Sometimes employers will have a trusted “gold standard” data set of “ground truth” answers — correctly classified cultural symbols. These data sets might be produced and validated by AMT (or similar) workers, or acquired from trusted projects, labs, or other public datasets (Stanford, Iriondo, and Shukla 2020). They can use this “gold standard” to test workers, slipping in tasks with known correct answers into a stream of tasks with unknown correct answers. Another strategy, detailed in a patent but also commonly discussed by engineers, can be summarized as “the most plural judgements”. This can mean simply assigning several workers the same task and using majority vote to decide on the “true” answer.

With both the “gold standard” test and the “plurality agreement” test, engineers face a tradeoff: the more “gold standard” test tasks or duplicated tasks, the greater the certainty that the workers giving the correct answers are actually trustworthy rather than lucky. But the more test tasks employers pay for, the greater the “human capital investment”. In patents and trade show presentations alike, engineers treat the confidence level needed in a worker a kind of knob that can be dialed up or down adding more or less information about workers. This additional
information can come by testing workers or gathering other information about them, such as through surveillance. The latter I will return to.

Assessing workers

Assessing human judgements can be a lot of extra work for engineers who have to put out multiple instances of a task, compare the answers, and figure out which workers to distrust or even blacklist. To reduce this work, Amazon has developed a program it calls “Masters.” Amazon promotes “Masters” workers as trusted producers of high-quality work and charges a premium for them. Masters workers do not earn a higher wage per task, but they get exclusive access to a large stream of work. Amazon makes “Masters” workers a default for employers setting up tasks on the platform.

Workers find the Masters designation puzzling and frustrating. There is no application process or clarity about the criteria to achieve this. You wake up one day and find out you’ve been chosen as a Master. On forums, workers will talk to each other to compare their statistics and try to decode why some get the designation and some do not. Excellent performance by the simple statistics workers get on the platform – the percentage of approved work tasks they’ve done, the number of tasks they’ve done – do not seem to predict getting the designation. What is interesting here, though, is that Amazon has developed a meritocracy among workers and its mechanisms are intentionally opaque, likely to prevent “gaming” by those imagined “bad actors.” (This is a world in which studying for the test is considered cheating.)

A 2011 Amazon patent holds some clues. The patent suggests that Amazon may calculate a “judge error rate” or confidence rating it assigns to workers behind the scenes (Figure 1). Amazon has an advantage over engineer-employers in that it can maintain a record of the workers’ error rates across their whole work history on the platform, across all employers. The patent suggests that Amazon, like engineers I’ve described, might use the kinds of “gold standard” and plurality techniques I described to evaluate “judges.” The patent suggests a wide range of qualities by which a worker may be evaluated, including accuracy, error rate, and speed of task performance.

While these may seem straightforward attributes of competence, the algorithm is agnostic to conditions that explain the differences, such as disabilities or multi-tasked care work in the
home. Turk workers work in varied conditions, in their homes, at the library, while at school. As independent contractors, this kind of flexibility is touted as precisely part of the appeal of gig work. But as Amazon judges the “judges”, these variations in bodies, environment, and work process manifest to the algorithm as differences in speed or even interpretive variations that manifest as “error rate.” Together, these can mean the difference between being algorithmically judged a Master or perhaps a fraudster.

An exception: finding a trusted pool

Once they have identified workers they trust, some engineers will develop custom lists of worker IDs they will clear for their tasks and treat this group as a trusted pool (Gray & Suri 2019). Some might create a Slack channel to communicate with these workers, or participate in worker-run forums to engage these workers through informal channels. These communication forums allow workers and employers to engage in more dialog about the labor process and how to adjust it. These more stable relationships might seem to indicate a tendency, as described by Ronald Coase, for firms to form as a way of decreasing transaction costs of operating on the open market (1937). These trusted pool formations reveal a tension, as argued by anthropologists Ilana Gershon and Melissa Cefkin, between neoliberal autonomy and transactional efficiencies. The emergent organizational forms reveal one way that workers and employers cobble together platforms and software, usually leaving platform operators like Amazon untouched, to negotiate these tensions in organizing a less wasteful and fairer labor process.

Such employers, from a workers’ perspective, are the exception. I show this exceptional form of collaboration to underscore how work organization could be otherwise from the approach to filtering and testing workers en masse. Why is it exceptional? Elsewhere, I’ve argued that part of the appeal of Amazon Mechanical Turk for engineers is that their managerial relationships and responsibilities are displaced into the technological platform (Irani 2015). Engineers describe feeling like the platform is “magic” because it allows them to focus on the coding work they are attached to, rather than the enactment of managerial authority that violates their image of Silicon Valley work cultures. Most employers want to keep their workers across the programming interface, out of sight to be filtered, transacted, and extracted.
Enforcing one login, one body

These techniques of assessing workers all depend on a one-to-one relationship between an Amazon worker login and the working body behind the screen. A login identifies the data object that holds the work history. When Amazon algorithms detect a possible violation of their assumption, they label accounts as at risk of being fraudulent. Workers only discover this when they get their accounts suspended.

One practice that Amazon penalizes is the sharing of a single worker login among several workers. This is a problem especially for Indian workers who often face barriers getting an AMT login. AMT does not accept all people who apply to be workers and, true to form for black boxed fraud governance, does not explain why they reject applications. It may be because Indian workers are less likely to be Amazon customers and thus lack a digital history, or it may be because Indian workers were more likely to be rejected by requesters for giving undesirable task responses and thus machine learning algorithms have learned to discriminate against workers from India in general. Some Indian workers unable to get their own account respond by sharing logins with others, working around the clock and dividing up the wages that accrue to the account. Amazon seeks to shut down this behavior that violates the integrity of one login, one body. Workers may suddenly find their accounts suspended, unable to access the previous earnings already held in their Amazon account.

Algorithms policing violations to one login, one body sometimes shut down practices that Amazon later determines, under pressure from workers, to be legitimate. In one case, a mother and son found their logins suspended because they were logged in from the same house, and thus the same wifi router, and, thus, had the same IP address. The accounts were only restored after Turkopticon worker organizers intervened to bring the case to an Amazon manager. Amazon explained their policy as a way of protecting the authenticity of social science research results. Amazon had interpreted the second login on the same IP address as a worker trying to get paid to do the same social science study twice, corrupting research results. While Amazon did admit its mistake when it reinstated the mother whose son turked from her home; for two weeks of lost earnings, they gifted her a $10 Amazon gift card far less than what she would have earned.20
Enforcing one login, one body means platform operators scan data flows in suspicion that one login hosts many bodies, as well as suspicion that multiple logins can host one body. Both are a problem for political economies of knowledge extraction. As Amazon’s algorithms automate fraud judgements, they may learn to simply exclude workers from Indian IP addresses, or IP addresses from Starbucks, or IP addresses from libraries in low-income neighborhoods without, as Burrell and Jonas argue, “understanding the systematic social and political conditions that produce differential behaviors online.”

The World’s Largest Fraud Detector?
The techniques described above are of consequence not only to Amazon Mechanical Turk employers and workers, but to internet users at large. While Amazon’s approaches to fraud remain opaque to outsiders (and likely even many insiders), the company has made its cloud-based Fraud Detector available as a platform service it sells to other organizations. This is significant for several reasons. First, it means Amazon disseminates its techniques to the internet at large. Second, Amazon becomes a central broker of data signals on users and can leverage data and risk assessments made for one client to inform assessments for another client. Amazon Fraud Prevention team lead Ryan Schmiedl described this bleed of risk data across sites as a “lift” clients get from Amazon: “we’re taking patterns from repeated bad actors...so you’re benefiting not just from what you know, but from what we know”.

Amazon’s Fraud Detector might label as higher risk whose self-declared country and customer address are different, or whose IP address country and phone numbers are different. A user facing precarity and moving across state and country borders, as is common between San Diego and Tijuana, here becomes suspect. Similarly, someone couch surfing in a different location than their listed address might be flagged. The machine learning algorithm, according to Schmiedl, also flags practices that are simply outliers “unlike anything it has seen from legitimate customers.” To be risky, then, is not to demonstrate threatening behaviors. It might simply be that one seems dissimilar to others represented in the dataset.

Fraud reduction can justify creative and expansive forms of surveillance. One patent (Figure 2) describes a data-thirsty technique that tracks user behavior habits, such as sequences of applications opened in the morning, combined with contextual markers such as location,
microphone data, and relationship to surrounding objects. That’s the “behavioral data collector” indicated in the patent figure. The system authenticates users when they are acting habitually, as discerned by the algorithm. When use patterns change, the system forces reauthentication.\textsuperscript{24} The patent claims an expansive range of surveillance modalities to protect the sanctity of digitized finance systems and firm financial flows. This patent also appears perfectly aligned with Amazon’s fight against people consensually sharing a single internet login.

Penalties for those informally labeled as “fraudsters” include loss of work, accrued wages, and even login-restricted services across the web. As a login infrastructure provider, Amazon controls not only access to its sites but access to all kinds of other sites across the internet.

Fraud risk techniques do not always present users with clear consequences. It can, according to Amazon presentations, result in “friction.” “Friction” can take many forms. It can be those CAPTCHAs that ask you to mark all the trucks, bridges, or stop signs in a set of images. It can come as requests for additional authenticating data (address, phone number, social security number). It can come as a temporary delay pending a customer service call. Friction allows Amazon to titrate caution against fraudsters against the desire to allow customers to pay them. When dealing with customers who purchase products, Amazon needs to balance potential costs of fraudulent activity against the costs of slowing or blocking revenue-generating customers. But when dealing with workers in Amazon Mechanical Turk, Amazon faces a surplus of interested workers and even turns applicants away.\textsuperscript{25} Thus, it can aggressively suspend long time workers or even block newer, untried workers with little consequence to the company.\textsuperscript{3}

**Governing algorithmic judgement**

Scholarship on algorithmic judgement has identified several distinct kinds of problems, each of which imply distinct resolutions or mitigation strategies. Amazon Mechanical Turk workers facing reputational harm and account suspensions can face problematic data, problematic engineering assumptions, problematic algorithmic inferences, or the criminalization of practices that are inconvenient for company business models. While the first two kinds of problems have been discussed widely in scholarship, the latter two have attracted less attention among those concerned with workers’ or consumers’ rights.
Rights to see and repair data about platform users

The simplest kind of problem faced by workers confronting account suspensions is the correction or updating of data. Workers, like financial service users, might be flagged when they log in from a location distinct from the address registered to their account. Unlike financial service users, however, workers rarely have the opportunity to set an updated location status on the platform to avoid getting flagged.

Legal scholar Frank Pasquale has called for policies that guarantee the right to review data records about oneself. The fraud algorithms that are the central concern of this chapter are a key element, I argue, of what Pasquale calls “the black box society” – a society in which opaque and automated surveillance and reputational judgements restrict one’s access to resources and activities. The right to review and correct data ensures one mechanism for contesting unfair judgements. Companies can be expected to resist such transparency, arguing that it would allow bad actors crucial tactical knowledge about the cybersecurity battlefield. However, cybersecurity researchers argue that a truly secure system is one that is robust against an adversary who understands how it is constructed. Transparency, conversely, improves security by expanding the community of people who can point out problems in the system and suggest mechanisms for repair.

Evidence from this chapter shows how the term ‘bad actors’ occludes unjust consequences of platform operator design, algorithms, and policies. For workers and users confronting algorithmic judgements, account suspensions exemplify an emergency – a moment when technical and social conditions create an unusual event. These events do not happen every day or even to most users. For this reason, data transparency ought not to place the responsibility for maintaining correct data on workers, adding an extra labor to the time they spend producing. Rather, it ought to be one means of mitigating harm in a larger process of repair when algorithms, like people, inevitably misjudge the social world and fail.

Beyond ethics education: oversight and accountability to those impacted

In some cases, patents reveal engineering assumptions that explicitly encode a model of knowledge or ability that reproduces hierarchies among difference. Recall, for example, the patent that assumed speed as one indicator of worker quality, ignoring differences in competing
obligations, pacing preferences, or body mobilities. Such an assumption seems especially unjustifiable on a platform in which workers are paid piece wages, rather than per hour. Such an assumption is also especially problematic given the propensity of computer work to produce repetitive stress injuries that might slow workers down.

Simply educating engineers in ethics or social science methods cannot address such gaps, though such education may make engineers more aware of the gap and the need to address it. Social justice approaches have focused on such assumptions and argued that those who design must do in ways accountable to those directly affected by the design. Drawing on a wide range of scholarship in feminist studies, disability studies, and the knowledge of social movement actors, such an approach draws on the knowledge of differently situated actors about the emergent effects designs may have on their lives. Technology transparency and oversight policy approaches require companies to reveal details of algorithms and data practices that affect users; they also create mechanisms of public regulatory oversight over platform operators, giving users one lever for understanding, redress, and advocacy.

These transparency and oversight approaches must not exempt fraud algorithms from rights and oversight claims, but some currently do. For example, California Assembly Bill AB-1790 sets out requirements for how online marketplaces such as E-Bay or Amazon resolve user disputes with what the law calls “minimum fairness,” including specifying in writing grounds for suspensions. Yet the law exempts the disclosure of “information that would hinder any investigation or prevention of deceptive, fraudulent, or illegal activity.” This exemption gives broad berth for platform operators to deny transparency and oversight to users. Another example of policy that exempts fraud algorithms was the California Privacy Rights Act (CPRA) of 2018, passed by the legislature, which required businesses to respond to consumer requests to delete their personal information. This law also offered exemptions for consumer data kept to detect “fraudulent…activity.”

**Shield platform users from systemic risks**

The problem of algorithms, Louise Amoore argues, is not only “the power to perceive, to see, to collect, or to survey a vast data landscape, but the power to perceive and distill something for action.” When algorithms of suspicion target a user for outlier behavior or behavior that pattern
matches prior examples of bad actors fed to the system, that person might find themselves snatched out of an ocean of users for reasons of correlation rather than observed malfeasance.

This algorithmic power to focus and make actionable based on correlation introduces a kind of systemic risk – a expansion of vulnerabilities as systems become more interconnected and complex.\textsuperscript{32} Algorithms draw on diverse sources of data through diverse modeling techniques being deployed and tested on people in their real lives, rather than in the lab. I argue that this generates an accumulation of risks in the platform management system, but the consequences of accumulated risk then is concentrated on those workers who find themselves suspended by mistake.

We need policies, norms, and practices that account for this risk and protect people from the harms such risks can generate. A simple example for Amazon Mechanical Turk workers might be estimating the lost wages from a mistaken account suspension based on past earnings and adding compensation duress and for time spent working towards resolution. Actual solutions should be developed in collaboration with those most directly impacted by these risks.

\textit{Refuse simple and criminalizing claims of fraud}

Algorithms of suspicion are not only harmful because their inferences or data are problematic. They can also be harmful by scanning for and targeting behaviors that might not be morally wrong but are inconvenient, undesirable, or costly for those who profit through algorithms.

To illustrate how socially acceptable practices might be inconvenient for and thus targeted by companies, I offer an example from the history of Google. When I worked for Google in the early 2000s, it was common for ad agencies to have a single login shared among staff to bid on Google AdWords keywords and craft ads. When Google transitioned the AdWords system onto the master Google Accounts system, we forced each agency worker to create their own login. Google wanted to impose an identity between login and person in order to collect individualized data and create profiles for “personalized search” and personally-targeted advertisements. (Prior to this, Google ads were contextual, based on what you searched for at that specific moment.)

Like Google, Amazon imposes an authenticated vision of an individual subject, penalized for interdependence with others and sharing of resources. The “wisdom of crowds” relies on the
people as sensors of their environments, and requires — in fact, enforces — their independence.\textsuperscript{33} It recasts collaboration – between mother and son, or workers in a cowork space – as collusion.\textsuperscript{4}

Part of the work of this chapter has been to denaturalize fraud and its associated discourse of “bad actors.” The meaning of fraud has shifted historically, from concerns about forged documents leading to improper property claims\textsuperscript{34} to concerns about compromising investors when uncertain statements about the future cross over into lies.\textsuperscript{35} The language and techniques of fraud I have traced here are less concerned with whether a person has documentary authority or is truthful, but rather whether they can be trusted as a cultural worker and, in turn, as an authority on legitimate cultural meanings. A worker who offers a less “popular” answer or an answer the employer does not consider sensible can be labeled fraudulent, rather than simply culturally different. On platforms, as in domains of public services in the United States, accusations of fraud can serve the goals of accusing organizations to evade responsibilities as part of a broader social contract.\textsuperscript{36}

**Conclusion**

What does it mean that fraud regimes are now being imposed on everyday communicational and work transactions, suppressing or even criminalizing other systems of ethics and truth such as care, cooperation, or infrastructure sharing? Further, Amazon is generating a market for fraud detection as a service, spreading practices drawn from finance, internet security, and international relations with their anxieties about bad actors who must be kept in the dark. In generating a market, Amazon generates desire and extends its infrastructures into new arenas of social life. In describing fraud detection systems, engineers easily slip into deploying quasi-criminalizing language that reframe a fraud risk as an individual as malicious and untrustworthy. Such an orientation forecloses avenues for recognizing harm to workers and other users, recognizing badly designed platform workflows, or repairing problematic data and algorithmic inferences. Finally, algorithms of suspicion generate systemic risk unaddressed by ethics approaches that focus on transparency and accountability. Such approaches do not account for how algorithmic management generate new kinds of uncertainty and risk and then concentrate impacts on the shoulders of just a few. We need policies, norms, and practices that
account for such risks and protect people from the harms such risks can generate and offer redress and compensation when an algorithm shuts them out.

Acknowledgements
I am indebted to helpful readings and discussions with scholars at AI Now, UCSD’s Critical Data Studies group, participants in an SSRC workshop on authenticity organized by Wendy Chun, linguistic anthropologists at the Michicagoan Conference, graduate students at Cornell University, and the Platform Governance volume editors. I also thank Stuart Geiger, Ilana Gershon, and Nick Seaver, and the editors of this volume for reading and discussing drafts of this work.

References

AB-1790.
https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB1790

https://escholarship.org/uc/item/0j88z94p.

https://doi.org/10.7551/mitpress/12255.001.0001.


Figure 1: Amazon patent “Authentication and Fraud Detection Based on User Behavior”


10 https://www.cloudresearch.com/resources/blog/mechanical-turk-data-five-years-in-five-figures/


17 Hullender, Evaluation of task judging results

18 Ibid.


22 Schmiidl, Tostenrude, and Suro, “AWS Re:invent’

23 Ibid.


31 Amoore, Cloud Ethics, 16.


General Comment

Amazon Mechanical Turk Workers lack accountability and redress when they are managed at scale, and by code. The AI industry is worth trillions of dollars, producing “scientific innovation” and “artificial intelligence” through the work of hundreds of thousands of data workers. Amazon operates a platform, Mechanical Turk (AMT), with workers from around the world, but the majority are in the United States. Researchers estimate that as late as 2019, there were at least 250,000 AMT workers worldwide. Like many gig work platforms, Amazon Mechanical Turk 1 asserts that workers are independent contractors. As a result, they don’t enjoy a minimum wage or occupational health and safety protections. The International Labor Organization found in 2016 that the majority of Amazon Mechanical Turk workers had a college degree or higher. Overall, 37% reported that it is their primary income.2

When Amazon launched the service in 2006, Jeff Bezos explained that engineers could use workers just as they might write a piece of computer code.3 Engineers can create jobs, set prices, and incorporate work output straight into their code from Application Programmer Interfaces (APIs). Today, the platform forms a key piece of Amazon’s machine-learning web services, such as the SageMaker platform. Workers experience a lack of accountability and redress in practice from those who hire them on AMT, or Amazon itself. Both Amazon and some researchers who rely on our work on AMT collaborate with and/or receive funds from the US federal government through the National Science Foundation and other research and technology development agencies. The following stories exemplify problems workers face when managed by code on AMT. Many of these problems are not so much consequences of the kinds of statistical artificial intelligence we hear so much about, but from complex layers of more familiar kinds of computer code that affect what work workers can access, whether or how they get paid, or whether they can retain their livelihoods through account access.

Turkopticon is not a union, but a worker-led group that advocates, organizes mutual aid, and creates resources to make AMT a good job while improving conditions for all workers.
Please see our attached report for workers' experiences of different issues that arise as they are automatedly surveilled and managed on the platform

Attachments

White House Managed by Code worker stories (2)
Managed by code: Worker problems on Amazon’s Mechanical Turk platform

By Turkopticon
June 27, 2023

This report, including research and analysis, has been compiled by Amazon Mechanical Turk workers and academic collaborators. For questions and follow up on these issues, please contact Lead Organizer Krystal Kauffman at policy@turkopticon.net.
Amazon Mechanical Turk Workers lack accountability and redress when they are managed at scale, and by code

The AI industry is worth trillions of dollars, producing “scientific innovation” and “artificial intelligence” through the work of hundreds of thousands of data workers. Amazon operates a platform, Mechanical Turk (AMT), with workers from around the world, but the majority are in the United States. Researchers estimate that as late as 2019, there were at least 250,000 AMT workers worldwide.¹ Like many gig work platforms, Amazon Mechanical Turk asserts that workers are independent contractors. As a result, they don’t enjoy a minimum wage or occupational health and safety protections. The International Labor Organization found in 2016 that the majority of Amazon Mechanical Turk workers had a college degree or higher. Overall, 37% reported that it is their primary income.²

When Amazon launched the service in 2006, Jeff Bezos explained that engineers could use workers just as they might write a piece of computer code.³ Engineers can create jobs, set prices, and incorporate work output straight into their code from Application Programmer Interfaces (APIs). Today, the platform forms a key piece of Amazon’s machine-learning web services, such as the SageMaker platform. Workers experience a lack of accountability and redress in practice from those who hire them on AMT, or Amazon itself. Both Amazon and some researchers who rely on our work on AMT collaborate with and/or receive funds from the US federal government through the National Science Foundation and other research and technology development agencies.

The following stories exemplify problems workers face when managed by code on AMT. Many of these problems are not so much consequences of the kinds of statistical artificial intelligence we hear so much about, but from complex layers of more familiar kinds of computer code that affect what work workers can access, whether or how they get paid, or whether they can retain their livelihoods through account access.

Turkopticon is not a union, but a worker-led group that advocates, organizes mutual aid, and creates resources to make AMT a good job while improving conditions for all workers.

When requesters “mass reject” work and workers

AMT workers describe “mass rejections” as a devastating but all too common event when a requester – the employer seeking data work – rejects every HIT (Human Intelligence Task) a worker has submitted, or a large number of them. Though Amazon permits requesters to do this, assuming that “rejected” and unpaid for work is bad work, there is no process on the platform to verify this. It is highly unlikely that all workers submitting work have submitted bad work; thus, mass rejections are usually understood to be bad faith acts by the requester. Rejections negatively impact the workers’ approval rating. This, in turn, limits the amount and quality of work available to the worker. Rejections stay on a worker’s record indefinitely, even when the rejection is unwarranted. To rebuild their approval rating, workers often have to take the least desirable, most poorly paying tasks until their rating improves and gives them access to better work.

“As a Turk, I experienced a mass rejection when I returned to MTurk after several years. I had an excellent rating that was quickly tanked after I completed many HITS for a requester who rejected all of them. I have had to work very slowly to rebuild my rating over the past six months. After completing thousands of HITS, my rating has not even made it back up to 99%. I haven’t had a single HIT rejected since experiencing the mass rejection. I try to be a careful and reliable worker, and at this rate, it may take me years, if ever, to recoup my rating. This limits what HITS I can qualify for and greatly reduces my options for work.”

“I’m new to MTurk (just started yesterday), and I first did 6 HITS by [requester], which were rejected. I did 2 more before I googled where the rejections were...all from [the requester]. I’m taking this as a learning lesson and have blocked [the requester] but now I need to get 7k or 8k approved HITS to bring it to 99%” (modified to anonymize)

“Seungho Kim, a requester, has been doing mass rejections for a while. I’m not certain why. I didn’t have a single one of mine approved out of I believe it was 57 HITS. From reading other reviews, it’s an ongoing issue...If I had those 57 HITS approved, I would not have had to work so hard just to get my approval rating up. I am not back to a 99% rating yet. I have 5k [tasks] until I get back to 99%. This mass rejection took me down to 96%...I reached out to this requester numerous times to hear nothing back.

If you see one of their HITs, it’s pretty easy, but they leave some questionable grey spots, I guess. I reached out to them and asked for clarification on what exactly I did wrong to understand what they wanted. (i.e., if I could see it was a tiger, but the image was blurry, is it okay even though it’s blurry and I can make it out?) I also asked if they would consider overturning my rejections. It has been, I believe, a month and a half since my rejections. I did not contact Amazon about this; honestly, I’m not even sure I know where to find their contact information for situations like this.”

2
In some countries, Amazon pays in company scrip

Amazon does not offer bank deposits to all workers, some are only able to redeem Amazon gift cards for their work – the same work that others get actual income from. While it appears to be based on workers’ country of residence, it is not always clear to workers why they are not able to be paid in actual funds.

“I started working on MTurk between 2015 and 2016, and since then, I have been waiting to be allowed to withdraw my earnings to my US bank account. To be clear, I’m not a US resident. I can only use my MTurk earnings on Amazon.com, and I’m trapped in an unending profit cycle for Amazon: first, being a Turker, and second, being an Amazon.com customer (not by choice). Besides, although I have an excellent approval rating (99.9% with +210K approved HITs) and follow all the rules and Terms of Services, I’m still afraid that my account could be unfairly suspended (like it has happened to other Turkers) and that I might lose all of my accumulated earnings throughout all of these years. To use my funds in real life out of the Amazon ecosystem, I’m constantly searching for members of my family and close friends who want to purchase products from the Amazon.com website so that I can buy these for them in exchange for their money. It’s unfair and unethical”
Outdated data can mean workers’ peril

Demographics are an important part of the Mturk platform. Amazon collects worker characteristics such as age, gender, race, and education (optionally) that open access to, or restrict, access to certain work. Certain personal information about workers, such as gender and location, cannot be updated in Amazon’s system. Workers understand this as a measure to prevent “scamming,” or changing characteristics to access work (e.g. surveys) meant for certain demographics. However, this prevents workers from legitimately updating their characteristics such as when they affirm their gender, or when they move homes. As a result, workers who transition cannot qualify for work based on their actual, current status. For example, a worker whose address changes sometimes cannot qualify for work based on their actual, current location.

When the platform detects a difference between recorded data and detected data, such as an IP address location and recorded address, it can also flag the worker’s account as suspicious. In some cases, this can result in worker account suspensions, blocking workers’ access to their accounts, their work, and their accrued earnings.

“...the fact that Mechanical Turk can’t/won’t update locations (which are used as a qual for many studies) seems to exemplify how little effort they put into the platform. There are numerous people who have mentioned this so I am not surprised that 16 months after I moved from VA to CA, mTurk still lists me in VA, despite my updating my account immediately (& ordering things to be delivered here)”
“Masters”: an “black boxed” algorithmic promotion that benefits the few

AMT has a system called “work qualifications” to allow requesters to control what kinds of workers have access to their work. Qualifications can include whether the worker is an iPhone or Android user, whether the worker has passed a particular skill test, or whether the worker has been named a “Master” worker by the Amazon Mechanical Turk platform.

Amazon’s “Masters” qualification has been a particular frustration for workers on the platform. Amazon assigns the qualification to workers without explaining what assessments of behaviors resulted in the assignment. Requesters are able to easily create jobs that only go to Masters workers on the Amazon Mechanical Turk website. Amazon explains the Masters qualifications to requesters as follows: “Mechanical Turk has built technology which analyzes Worker performance, identifies high performing Workers, and monitors their performance over time. Workers who have demonstrated excellence across a wide range of tasks are awarded the Masters Qualification. Masters must continue to pass our statistical monitoring to retain the Mechanical Turk Masters Qualification.”

Most workers never get the Masters qualification, even when they have performed tens of thousands of tasks at extremely high rates of approval. Workers are also unsure if Amazon is even qualifying workers as Masters anymore, despite offering the qualification filter to requesters on the platform as a way to ensure high-quality workers. Since 2019, Turkopticon has not heard self-reports of new workers attaining this status on the platform. Amazon has never explained who gets the qualification or why they choose not to give it to others.

Many requesters believe that Masters automatically means higher quality data, which isn’t necessarily the case. It only restricts workers from accessing their work dramatically. We argue that there are better ways for requesters to get quality data without excluding so many workers. Better methods that are more transparent to workers, such as total HITs completed by the worker, higher approval ratings, or “closed quals” — skill-specific tests requesters can have workers pass before hiring them on.

“It is understandable that the master’s qualification should be earned, but there is no way to know how, and unfortunately because it is offered without any real explanation of what it is, good workers who would otherwise be qualified to complete tasks do not get the opportunity to complete them.”
Worker A: In fairness, the fact that Masters hasn’t been granted in years should make researchers think twice about using it as a required qualification.

Worker B: I don’t think Amazon should offer it to researchers!

Worker C: I think it’s more the labeling. They think they’re getting something premium like when products put labels on their packaging that say "New and Improved" when the only thing new is the label.

Worker D: ...Since Amazon charges them to use quals, I doubt seriously [that] they’re being told that it’s not as useful a qual [qualification]... Researchers (especially new ones, but seasoned ones too I would imagine) see "Masters" and likely think "oh, great -- better quality responses ... lemme use that real quick". :confused:

... 

Worker Z: a lot of times they will end up removing the qual and reposting without it, so that goes to show it really does not help

Worker E: For them? No. For Amazon, yes, because Amazon gets a cut for the masters queue. [The worker is referencing the fact that Amazon takes a higher fee from requesters when it connects requesters to Masters workers.]
Account suspensions: fired by algorithm

Amazon develops algorithmic supervision of workers by using feedback from job posters who have incentives and unchecked to punish workers for unsatisfactory work. Workers flagged by algorithms find themselves locked out of their accounts with no explanation.

What makes a worker suspicious to algorithmic management used by Amazon or requesters? First, requesters can withhold pay for work they do not like or understand and this, in turn, lowers workers’ approval rating on the platform. Amazon's patents also suggest that the platform also rates workers by subjecting them to hidden tests and comparing their answers to other workers. Employers often fail to train workers to produce the kinds of results they want, and offer no pathways for workers to repair mistakes or misunderstandings. Workers lack formal processes for contesting these evaluations and associated wage theft. Amazon then uses these evaluations – job poster pay withholding and hidden tests – to develop machine learning models that guess whether a worker is a “bad actor.”

One worker Turkopticon helped had lost her account and access to her earnings, stored on the platform, for two weeks over what Amazon later admitted it was a mistake. The platform’s algorithm flagged her account because it detected two people – her and her son, it turned out – logged in and working on the same wifi network. It may also be the case that the algorithm had “learned” that low quality workers shared wifi and flagged the account. On her suspension, the worker appealed to Amazon but got no response until Turkopticon, a Turk worker organization, approached Amazon collectively. Only then did Amazon re-investigate and admit that it made a mistake. An analysis of Amazon patents reveals that Amazon uses a surveillance of a wide range of behaviors to decide whether to trust the worker logged in behind the screen – a worker they will almost never meet – or to suspend them.

---

My name is (b)(6) PII, and I work as an outbound packer at the Amazon STL8 Fulfillment Center in St. Peters, Missouri. I am also a member of the STL8 Organizing Committee and the Missouri Workers Center, which I joined to fight for higher wages and safer work at Amazon. I am also a single mother (b)(6) PII

Amazon knows every move I make from when I enter the turnstile to when I walk back out at the end of a shift. Amazon cameras track me from my work area all the way to the bathroom. They know when I go in and when I go out.

Amazon has cameras in the parking lot, in the entryway, and every six feet along the walkways throughout the building. They track me from the moment I get out of my car. At most stations there are 2-3 cameras watching my every move.

If the cameras weren’t enough, Amazon measures my performance down to the second. Management monitors three things while I’m working. As soon as I scan into my work station the clock starts. I work in multi-pack, which means I pack boxes with multiple items. I scan each item that goes into the box, and each box I complete packing. Amazon tracks my rate, or the number of items I scan per hour. They also track my TAKT time, or my time between each scan. Finally, they track our Time Off Task, or “idle time.” If I don’t scan an item for a few minutes, for example if I have to go to the bathroom which can take me ten minutes to walk across the facility, they log my time as time off task, regardless of what my rate is. In other words, you could work faster than anyone in the facility, but if you have too much idle time you can still be written up.

Let me explain to you my job this way:
Grab and build box 10 seconds
Identify and move to chute 4 seconds
Grab scan and place items in box 14 seconds (that could be from one item up to 50 items)
Pull dunnage into box 3 sec
Scan Amazon tracking label and tape box close 4 sec
Place box on line 2 seconds
Full process for each box - no more than 37 seconds
Start over There’s no down time,

I do this job 180 times an hour for six to ten hours a day That’s over 5000 items a week And by the way, our hourly task rate does not get adjusted if we need to use the bathroom outside of break times—the rate clock doesn’t stop running which means I am literally running across a big facility to the bathroom and back, and then speeding up when I return in order to make up for lost time.

As I mentioned before, (b)(6) PII
required to stow
250 items per hour (regardless of their size or weight.)

(b)(6) PII
required
to pick 350 items per hour

After working a shift, I come home exhausted and ready to fall into bed, but as a mother I can’t do that One of our cars is broken down right now, so after I come home from working the day shift, (b)(6) PII

On October 6th of last year, I was packing a case of sparkling water (b) (6)
My manager sent me to AmCare, Amazon’s in house medical They gave me ice
(b) (6) When I came back to work the next day they wanted to send me back to my station immediately (b) (6) I demanded to see a doctor. After getting the runaround from Amazon’s workman’s comp doctor, although the OSHA log I received from Amazon makes no mention of this. (b) (6) Amazon sent me back to work without an accommodation

The work that me (b)(6) PII at Amazon is not unique, (b) (6) I experienced, nor the company’s callous disregard for my health. We have a joke (b)(6) PII that the only time there isn’t an ambulance out front is when we’re closed for the day But safety at Amazon isn’t a joke, and given the thousands of injuries and even deaths workers have witnessed over just the last year, Amazon needs to take worker safety seriously

Amazon’s motto is to be the world's best employer, and we want to hold them to that standard I’ll go even further: Amazon has the resources and ingenuity to run the safest warehouses in the world, and that’s the standard to which they should be held
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0192
Comment on FR Doc # 2023 12995

Submitter Information
Email: [redacted]
Organization: National Domestic Workers Alliance

General Comment
See attached file(s)

Attachments
6-22-2023 National Domestic Workers Alliance Response to RFI OSTP_FRDOC-0001-0004 (Worker Surveillance and Management)
June 29, 2023

Submitted via: https://www.regulations.gov/commenton/OSTP_FRDOC_0001-0004

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
725 17th Street NW
Washington, DC 20500

Response to Request for Information
Automated Surveillance and Management
Docket ID: OSTP_FRDOC_0001
Federal Register Number 2023-09353

Dear Office of Science and Technology Policy:

The National Domestic Workers Alliance ("NDWA") appreciates the opportunity to submit the following information in response to the Request for Information: Automated Worker Surveillance and Management, Docket ID OSTP_FRDOC_0001-0004, Federal Register Number 2023-09353 published on May 2, 2023 ("RFI"). This letter provides information about GPS-based surveillance of house cleaners, nannies and direct care workers, camera surveillance of nannies, and malfunctioning app-based clock and and clock out automated systems that impair direct care workers from providing high quality care.

BACKGROUND:

The National Domestic Workers Alliance (NDWA)1 is the nation’s leading voice for dignity and fairness for the millions of domestic workers in the United States. Founded in 2007, NDWA works to raise wages and strengthen industry standards to ensure that domestic workers achieve economic security and protection, respect, and dignity in the workplace. NDWA organizes domestic workers, cultivates the leadership of low-income women and women of color, leads campaigns at the federal, state and local levels for policy change, and engages in workforce development and social innovations to deliver greater economic opportunity and security to domestic workers. We reach and engage over 400,000

1 https://www.domesticworkers.org/
domestic workers on a regular basis through our 70 affiliate organizations, local chapters, and online network across 50 states.

NDWA applauds the Office of Science and Technology Policy for requesting information about the impact to workers and workers’ rights of automated systems that monitor, manage and evaluate workers. NDWA has heard from numerous domestic workers about the negative impacts of these systems. This response will provide information about automated systems used in the employment of house cleaners, nannies and direct care, and then provide recommendations as requested on policy approaches.

**House Cleaners**

There are a number of gig work apps which pair clients seeking house cleaning services with house cleaners, such as Homeaglow, TaskRabbit, AllBetter, MaidsApp, Tidy, Housecall Pro and Extra Cleaning App. Some apps track them using a Global Positioning Satellite (GPS) component which tracks the location of the phone.

These apps also surveil and control communications between workers and clients, but do not provide enough access to workers to assert their rights. The apps have a strong incentive to prevent “disintermediation” - the communication of workers and clients outside the platform, as work contracted outside the platform will not result in a fee for the app. These fees are a large part of the business model, as well as the reason that venture capital is so attracted to these types of companies. In addition, app workers report losing access to the app and therefore to all previous communications upon an alleged violation of the terms of service. But the tight control causes problems for workers. Losing access to the communication system puts workers at a disadvantage in defending themselves against claims of being late, not completing work, not following instructions, or in liability claims that may arise in the case of accident or injury. For example, in its 2018 report, *Beyond Disruption: How Tech Shapes Labor Across Domestic Work & Ridehailing*, Data & Society relays the story of Tye, a Latina woman in her 20s who worked on a house cleaning app. After one job, she forgot to return the client’s key to a lockbox. Tye hoped to return the key as soon as possible, but once the job was over, the app no longer allowed her to see the client’s home address. By the next day, Tye had already been terminated from the app because the client had reported that the key had not been returned. Tye spent the next two months attempting to reactivate her account, losing out on income in the meantime.\(^2\) The obsession to keep workers and clients from communicating with each other outside a narrow window resulted in loss of job opportunities and income for the worker and inconvenience to the client.

Some house cleaning apps use automated management systems to rank workers and to decide which workers to display more prominently to more potential clients. TaskRabbit, for example, has an “elite”

---

status, which is achieved, in part, by accepting lots of jobs from the platform.\(^3\) Workers report that accepting or not accepting jobs affects elite status and other rankings on the site, even when accepting a job would be against the TaskRabbit Terms of Service or the client has underestimated the time for the job. TaskRabbit may be using automated systems to decide rankings. Reddit user “newrabbit” reported that when they turned down two jobs they went from 90% in the standings to 11% and dropped several places down in all searches.\(^4\) The worker had good reason for turning down those two jobs. The first, the worker reported, was to deliver alcohol, which the user reported is against the TaskRabbit Terms of Service. The other job presented a common problem workers report - mis-scoping. The client stated that they had hoarding disorder but booked only “regular cleaning” and not “deep cleaning.” The worker estimated that the job was very likely mis-scoped and would take longer than estimated. Workers risk having lower ratings for leaving mis-scoped jobs that they did not allot time for, or for taking longer and costing more than the client expected, due to erroneous (and possibly automatic) time estimates. Having a low rating and turning down a job, even a mis-scoped one, affects a worker’s appearance in the rankings, and thus ability to secure additional gigs.

Workers also report that these apps are amassing a huge amount of data about them and it is not clear to the workers how the data is being used, whether it is being monetized and sold, for example. NDWA surveyed 233 nannies, home care workers, and house cleaners. The vast majority said that they do not understand how app companies might be using their personal information or data. And the vast majority said that they were “very concerned” about the ways in which app companies might be using their personal information or data. The “terms of service” in these apps are usually very long, difficult to understand, and frequently available only in English,\(^5\) despite the fact that some gig workers have limited English proficiency.\(^6\)

On the positive side, Handy Technologies, Inc., dba Angi Services (“Angi”), has entered into an agreement with NDWA Gig Worker Advocates, an organization founded to advocate on behalf of domestic workers in the gig economy, which creates a formal process whereby house cleaners on Angi can discuss working condition concerns directly with decision-makers at Angi Services. The program is established and enforced by a private agreement and enforceable by contract law.\(^7\) The program is focused in Kentucky.

---

\(^5\) See, e.g. Homeaglow.com (Last accessed June 21, 2023) (showing Terms of Service for the U.S. & Canada only in English); Allbetterapp.com (Last accessed June 21, 2023) (showing Terms & Privacy Policies only in English).
\(^7\) Ai-jen Poo and Dawn Gearhart, “Domestic workers have long been underpaid and underappreciated. It’s time we give them what they deserve,” CNN Business, June 17, 2021. Available at
Indiana and Florida. This can serve as an example to other platforms, workers, unions, regulators and legislators.

**In-home Child Care Workers/Nannies**

In-home child care workers, commonly referred to as nannies, are being surveilled by their employers using a variety of old and new technology, along with vigilantism aided by technology. Nannies in the NDWA New York City chapter have reported that their employer has required them to install tracking apps on their personal phones as a condition of employment. Nannies have little insight into the data and the time parameters of these apps. They are likely having their location tracked during hours they are not at work. In addition, these apps likely track location during legally-mandated rest and meal breaks, despite the fact that for a meal break to be unpaid and legally count as a meal break, workers must be free to be completely relieved of work under federal law, and under some state laws, to leave the premises and do as they like. Some employers track their nannies entirely without their knowledge, by, for example, dropping a keychain-sized Apple AirTag tracking device inside a child’s diaper bag or stroller. Some nannies report being unsure whether these apps are also tracking their phone calls in and out, text messages and other communications on their personal phones.

NDWA has helped domestic workers who were subjected to forced labor and trafficking, especially live-in domestic workers from isolated mansions, and the first thing the workers do is throw out their phone, because they are so fearful that they are being tracked using the phone. Some domestic workers are so monitored by their employers, that they are unable to get information about basic human supports such as medical care or social groups. Often the first time an organization such as ours hears from such a worker is when they are in physical danger or have been evicted from their living quarters. Workers have also contacted NDWA using the phone of a friend or stranger because they are fearful of the unknown surveillance happening on their phone. This obviously interferes with a workers’ right to vindicate their rights under a variety of federal, state and local laws, including the wage payment laws such as the Fair Labor Standards Act, and anti-discrimination laws such as Title VII of the Civil Rights Act of 1964 and the New York Domestic Worker Bill of Rights.

Nanny-cams are not a new technology, but problems persist. Nanny-cams are hidden cameras that record video and sound at all times. Nannies report that nanny-cams are placed in private living quarters

---


8 Id.


10 29 C.F.R. sec. 785.19.

11 See, e.g. Washington Administrative Code sec. 296-126-092(1) (stating that meal periods must be paid if the employee is required to remain on the premises or at a prescribed work site).

12 Apple, AirTag. Available at https://www.apple.com/airtag/ (Last accessed June 8, 2023). (Describing how one can track the location of an AirTag using the “Find My” app on an iPhone.)
of live-in domestic workers, causing significant privacy violations. Nanny-cams also are likely not turned off during the meal or rest breaks that are legally mandated in many states,\(^\text{13}\) or when a nanny is otherwise outside of work hours.

“Nanny vigilantes” use a wide range of apps such as NextDoor, as well as Facebook Groups, such as “moms” Facebook groups. A vigilante will observe a nanny engaging in some alleged infraction, take a photo (rarely a video, frequently causing actions to be taken out of context) without permission, post it without permission with a phrase such as “Is this your nanny?” Such posts often result in nannies being fired without due process and getting blacklisted from being hired at all in an entire city. In one recent example, a nanny, who was a person of color, brought a child onto a New York City bus in a stroller, and did not unfold the stroller. A vigilante took a picture and posted it on social media, causing a firestorm of disapproval of the nanny for allegedly violating the norms of New York City life where strollers must be folded on a bus. However, a recent law change allows open strollers on city buses.

**Direct care**

Medicaid is the federal-state health care system for low-income people. The 21st Century Cures Act passed by Congress in 2016, mandates that all Medicaid personal care services and home health services have Electronic Visit Verification (EVV).\(^\text{14}\) Many state agencies which implement Medicaid-funded programs are requiring direct care workers (also referred as “home care workers”) providing such services, to use apps with automated surveillance and management to track visits. The most common app is provided by the Sandata company.\(^\text{15}\) As of 2022, EVV systems were in place covering an estimated 4.8 million low-income children, adults, and older people with disabilities.\(^\text{16}\) These apps require workers to clock in, clock out and sometimes check in mid-shift using a smartphone app. Federal legislation requires these systems to remain “minimally invasive,” but there is no specific guidance on this.\(^\text{17}\) These apps have resulted in wage theft. In Arkansas, one worker received only four days' notice of the EVV rollout and was not able to receive all the required information by the time of the rollout. The consumer this worker was caring for shelled out hundreds of dollars to purchase a smartphone for the worker. The worker attempted to use the app, but it was glitchy. The manual was 43 pages long, and only two training sessions were offered before the rollout. One timesheet was denied for “insufficient funds” and the worker lost out on $900 in wages, which the low-income consumer then paid out of his own pocket. The Arkansas Medicaid-implementing agency acknowledged, “When we went live…with the EVV

---

\(^{13}\) See U.S. Department of Labor Wage and Hour Division, Minimum Length of Meal Period Required under State Law for Adult Employees in Private Sector 1, January 1, 2023. Available at https://www.dol.gov/agencies/whd/state/meal-breaks (Last accessed June 21, 2023). (Showing some 20 states and territories with meal break requirements including Nebraska, Tennessee, Kentucky, and West Virginia.)


\(^{16}\) Shestack, EVV Surveillance.

\(^{17}\) Shestack, EVV Surveillance.
system...there were more issues than we anticipated.”

Another worker couldn’t access the system for two weeks and her paycheck was three weeks late, a violation of the Fair Labor Standards Act’s prompt payment requirement. The system had red-flagged all 16 of her shifts, while in the previous 13 years she had only had two shifts red-flagged.

Some EVV apps use “geofencing” to establish a minimum distance around a client’s home inside which a care worker is allowed to clock in and out without getting flagged as noncompliant. Before the use of this automated surveillance and management system, one Arkansa caregiver and consumer were always on the go - to therapy, grocery shopping and to see friends. But because of the geofencing, the worker said, “Now we can’t [do these things]. You have to be at home to clock in and clock out.”

A National Council of Independent Living survey found that one-third of respondents in 36 states said they stay at home more often than prior to EVV use, due to fear that geofencing limitations will flag a visit as fraud or cause delay in or loss of provider wages. Workers and consumers tend to stay close to each other and so these apps are tracking Medicaid consumers, raising health privacy and other privacy and autonomy issues as well.

In addition, direct care workers report that clocking time with the app takes significantly more time and attention than the previous method of a paper sign-in sheet. One worker in Arkansas reported that she had to clock in and out of the app as often as four times a day and on a fixed schedule, even though the consumer is supposed to get care whenever needed. This worker told the agency, “What took a total of 15 seconds - to sign a timesheet and submit to [the employer] - now takes many hours; hours that should be given to the client for care.” Thus, the app creates concerns for both consumer safety and worker safety. Many consumers who receive care and services under Medicaid are severely impaired and require constant care and vigilance. Turning one’s attention even for a few minutes to a cumbersome app compromises consumer and worker safety. If a consumer slides out of a chair while unattended, this creates a risk to the consumer’s safety, but also to the worker’s safety as the worker must now exert significant effort, nearly always alone, to return the consumer to safety.

One attempt at promoting worker voice in EVV was stymied by the federal government. In California, the labor union United Domestic Workers and Disability Rights California collaborated with consumers, workers and state officials to design an in-house EVV system that did not collect GPS data or require workers to log their hours in real time. But the federal government said this system was not compliant.
Policy Recommendations

As a result of the foregoing, NDWA recommends the following changes in policy, regulations and practices:

● Encourage or mandate companies using automated systems to surveil and manage workers to use these same systems to allow workers to submit concerns and quickly resolve disputes. In other words, if a company is going to make a particular communication platform mandatory for workers, then there should be a standard set of protections for workers to have access to those communications, even if they are “kicked off” the platforms, and a way to use those systems for workers to submit concerns to the company.

● Increase regulation and enforcement of misclassification of employees as independent contractors, which is rampant on many platforms that use automated systems to surveil and manage workers. The surveillance and management of workers is in fact proof of one of the important prongs in many legal tests of what makes an employee versus an independent contractor - control. All labor protection agencies should publish regulations that reduce the number of workers who are misclassified and commit enforcement resources to this pervasive problem. When workers are misclassified, it adds an additional hurdle to vindicating their rights to concerted activity and collective bargaining under the National Labor Relations Act, to minimum wage and overtime under the Fair Labor Standards Act, to occupational safety and health, workers’ compensation for on-the-job injuries, indemnification by their employers for accidental injuries and damage caused to others, and many other important rights.

● Encourage and mandate a “pay first, resolve later” system, where companies should pay workers their promised amounts or wages first, and resolve disputes and recover overpaid funds later.

● Encourage or mandate full worker access to all information held by the company before, during and after employment, especially during disputes over pay or other conditions of work.

● Encourage or mandate itemized statements that disclose hours worked, money earned and fees and penalties charged.

● Labor protection agencies should create “Terms of Service” and “Algo” teams. The Terms of Service Team will specialize in reviewing the terms of service of companies that use automated systems to surveil and manage workers. Where violations of labor law are found embedded in the terms of service, the agencies should open investigations and issue findings that the terms of service should be changed and that failure to do so will result in penalties. The Algo Team will specialize in obtaining and reviewing algorithms that affect workers. When violations of labor law are found embedded in algorithms, the agencies should open investigations and issue findings that the algorithms should be modified.

● Each federal labor protection agency should create a department or task force dedicated to monitoring privacy violations and developing targeted enforcement against repeat offenders. Repeat offenders should be required to register with each labor protection agency and share data about their employment practices, such as the number of worker complaints and type of violations found.

● The National Labor Relations Board should, by regulation or legal opinion, make clear that off-the-job surveillance (including during meal and rest breaks) is unlawful.
- The Department of Labor should issue a memo or other policy statement (such as a Wage and Hour opinion, Solicitor’s memo and blog post) similar to the one issued by the NLRB General Counsel26 spelling out its position on what automated surveillance is permitted and not permitted under the laws DOL enforces (such as the Fair Labor Standards Act and the Family and Medical Leave Act), especially when it comes to retaliation against workers for asserting their rights under labor laws. Such policy statements and guidance from the Department of Labor is especially important for domestic workers since they are excluded from coverage under the National Labor Relations Act.27
- Encourage or mandate easy-to-read terms of service labels on issues of worker surveillance and management, similar to nutrition labels and truth in lending labels. The label should be placed at the beginning of the terms of service and should include Yes or No answers to questions such as Will I be surveilled? Will I be surveilled outside of work hours? In the case of a dispute, will I have access to all information held by the company?

Please do not hesitate to reach out with any questions regarding the information provided. I can be reached at [redacted].

Again thank you for collecting this information for the good of workers.

Sincerely,

(b) (6)

Haeyoung Yoon
Senior Director of Policy and Advocacy

---

26 National Labor Relations Board General Counsel Jennifer Abruzzo, Memo: Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights, October 31, 2022. Available at https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and (Last accessed June 19, 2023). (Stating that “absent proper justification, the photographing of employees engaged in protected concerted activities violates the Act because it has a tendency to intimidate”, that surveillance of concerted activities is unlawful whether done covertly, overtly, or after the fact (by reviewing security camera footage, for example), and that employer’s interests in electronic monitoring and automated management must be balanced against employee rights.

PUBLIC SUBMISSION

**Docket:** OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

**Comment On:** OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

**Document:** OSTP-TECH-2023-0004-DRAFT-0193
Comment on FR Doc # 2023 12995

---

**Submitter Information**

**Email:** [removed]
**Organization:** Communications Workers of America

---

**General Comment**

Please see attached.

---

**Attachments**

2023.06.29 CWA Response to OSTP RFI on Automated Surveillance.docx
June 29, 2023

FR Doc. 2023–12995

To: White House, Office of Science and Technology Policy
   Executive Office of the President
   Attn: Alan Mislove, Assistant Director for Data and Democracy
   Eisenhower Executive Office Building
   1650 Pennsylvania Avenue
   Washington, D.C. 20504

Re: Request for Information on Automated Worker Surveillance and Management

The Communications Workers of America (CWA) respectfully submits these comments in response to the White House Office of Science and Technology Policy (OSTP) Request for Information on Automated Worker Surveillance and Management, dated May 2, 2023. We thank the OSTP and the White House for soliciting the views and experiences of workers who have been impacted by new forms of automated surveillance and management in the workplace.

CWA represents workers in private and public sector employment in telecommunications, customer service, media, airlines, health care, public service and education, manufacturing, tech, and other fields.

These comments are responsive to questions 1, 4 and 5 of the OSTP Request for Information, focusing on the experiences CWA-represented call center workers have had with new automated surveillance and management technologies and their impact on job quality. These comments will also summarize empirical evidence of surveillance technology impacts on workers in call centers across the United States. CWA-represented call center workers report the widespread use of Artificial Intelligence or algorithmic tools used for surveillance and management. These tools are associated with negative outcomes including the speed-up of work; expanded monitoring and discipline associated with surveillance; increased workplace stress; and lower job satisfaction. CWA-represented call center workers report instances of biased and unreliable analysis produced by these automated tools that highlight the importance of union representation and human oversight to protect against unfair outcomes.

As we will describe below, CWA members experienced firsthand how the COVID-19 pandemic accelerated the use of new technologies that have enabled companies to expand monitoring of workplaces and workers. The market research firm Gartner has estimated that 60% of large employers used workplace monitoring tools in 2021, double the amount used before the pandemic.\footnote{Jo Constantz, 'They Were Spying On Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions, NEWSWEEK (Dec. 13, 2021), https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603} A study of internet search terms by security and digital rights firm Top10VPN found...
that global demand for employee monitoring software was 54% higher from March 2020 to March 2023 compared to 2019. Even without specialized software, common office software can be used by managers to track data on employee work activities, movements and even worker sentiment and stress levels.

Employers have used this expanded surveillance to enable automated management systems to speed up the pace of work or otherwise control aspects of work performance, enforce productivity or other kinds of metrics, and violate workers rights to form a union and collectively bargain. Workers across a diverse range of industries and in jobs ranging from warehouse associates, social workers, lawyers, and hospice chaplains have seen the introduction of productivity monitoring systems that are used to enable automated decision-making regarding worker evaluations, compensation, discipline and retention. Workers under these automated management systems report that these systems often result in wage theft, discrimination in the workplace, and stressful work environments.

Policy makers should take action to strengthen protections for workers’ exercising their right to organize and bargain collectively over the adoption and use of new technologies in the workplace, including increased penalties on employers who violate labor law and use new surveillance tools to interfere with protected concerted activity. Federal action is also required to enshrine the principles of the Administration’s “Blueprint for an AI Bill of Rights” into law, providing transparency, recourse, human oversight, data privacy and protection from discrimination to workers and the public.

1. Monitoring and other technologies associated with increased management control have a negative impact on job quality and mental health for call center workers.

CWA represents 40,000 customer service workers, predominantly employed in the telecommunications industry, but also in airline reservations, public service, and other sectors. CWA-represented workers in call centers and in work-from-home positions perform a variety of functions including inbound and outbound sales, technical support, customer retention, dispatch, and collections.

CWA has engaged in a long-term partnership with scholars at Cornell University and McMaster University to survey and interview workers to better understand how management practices and

2 Simon Migliano, Employee Monitoring Software Demand up 54% since March 2020, Top10VPN (May 4, 2023), https://www.top10vpn.com/research/covid-employee-surveillance/
4 Constantz supra n. 1
7 Id.
technologies impact job quality in call centers. From December 2022 to February 2023, CWA and our university partners undertook a survey of call center workers on new Artificial Intelligence tools in the workplace, which will be described below. This new survey updates and affirms the findings of a 2017 survey of CWA-represented call center agents, which found that call center workers are subject to widespread and persistent monitoring to enforce performance metrics, including sales goals, call handling time and adherence to work processes that are unreasonable. Management monitoring of call center agents can take multiple forms including voice recordings, computer screen shots, tracking of keyboard strokes, and monitoring of text interactions. Call center agents reported that they experienced three different types of monitoring on average, with voice recordings reported as the most common monitoring tool.

The 2017 survey found that stress was a widespread issue among call center workers, with 87% of respondents reporting high or very high stress levels among their coworkers and 77% reporting high or very high personal levels of stress. Over 50% of agents reported having been prescribed medication to treat a stress- or anxiety-related illness or condition, with 24% reporting constant use of these medications. These rates exceed national averages of anxiety disorders, estimated to affect 19% of US adults by the National Institute of Mental Health.

Management control through monitoring of work and reduced agent discretion were found to be correlated with stress levels and employee burnout. Among those reporting very high stress levels in their call centers, the average number of monitoring methods was 3.2, compared to 2.6 for those reporting low stress. Among agents reporting very high stress levels, 22% had calls monitored by their supervisor once to several times a day, compared to 8% of those that report low stress levels. This frequency of monitoring is much higher than was typically reported. The majority of survey respondents (60%) reported their calls monitored several times a month or less.

The survey found that union representation is correlated with reduced stress – respondents reporting low stress levels were more likely to report that their union was helpful in addressing scheduling predictability, fairness of performance monitoring, and training quality and quantity. This has been an important area of bargaining for CWA members, who have fought for and won protections in our collective bargaining agreements against abusive monitoring, the speed-up of work, and unrealistic sales goals.

---

8 Virginia Doellgast and Sean O’Brady, Making Call Center Jobs Better: The Relationship Between Management Practices and Worker Stress, CORNELL U. (June 2021), https://ecommons.cornell.edu/handle/1813/74307
9 Id. at 24-25.
10 Id. at 3.
11 Id.
13 Supra n. 8 at 53.
14 Id. at 54.
15 Id. at 26.
16 Id. at 57.
2. The use of AI-based tools for automated monitoring and management is widespread among firms that employ customer service agents.

Artificial intelligence tools have been widely adopted across the call center industry, accelerated by the COVID-19 pandemic and the transition of workers out of traditional call centers and into home-based customer service work.  

The new AI tools are used for a range of functions, including the automation of customer service work (such as chatbots and virtual agents), the automation of management functions (including training, scheduling, and monitoring), and robotic process automation which supplements the work of customer service agents (including call routing, automated form population, and tools that automate technical support functions).

AI tools have also been used to expand and automate surveillance and monitoring of call center agents. “Sentiment analysis” tools record every interaction between customer service representatives and customers, providing real-time feedback to representatives regarding the pace of conversation, their tone of voice, and displays of empathy. Under one such system called “Cogito”, supervisors have instant access to a “CX Score” produced by this system for every call, purported to be an objective measure of customer perception of a call. Cogito Corporation describes this software as having “the ability to analyze the voice to understand a speaker's emotional state and deliver recommendations to steer the conversation.”

The business services corporation CallMiner bills itself as “the leader in conversation analytics” and markets its platform to call center operators as a tool that “analyzes interactions at the deepest levels, interpreting nuance and identifying patterns and traits that shed light on new areas of opportunity.” Employers use CallMiner to evaluate call center workers on measures including whether they were empathetic in their tone and used the proper call flow.

Speech emotion recognition systems such as Cogito and CallMiner rely on training data categorized into discrete emotions, an underlying framework that has been criticized for lacking scientific rigor.

---

21 The Stakes of Human Interaction Have Never Been So High, Cogito, https://cogitocorp.com/emotion-conversation-ai/
22 About Us, CallMiner, https://callminer.com/our-company/about-us
AI tools are also used to adhere agents to scripts, tracking and flagging deviations or missed keywords in real time. One such software in use at CWA-represented centers is called HiPer Agent Experience and is sold by XSell Technologies. XSell Technologies promotes their ability to “augment agents with AI-powered, real-time coaching, progress tracking, and our unique objection handling technology.” Objection handling consists of “AI-powered conversational paths” providing real-time scripts and coaching to agents which “overcome objections, anticipate opportunities, and increase customer interaction value” through increased sales.\(^{24}\)

AI tools, when paired with webcams, are also used to surveil employee workspaces and persons. One such system used by Teleperformance, one of the world’s biggest call center outsourcing companies, uses a program to scan the work area of home-based agents automatically and randomly for breaches of work rules and is enabled with facial recognition to confirm the identity of the agent.\(^{25}\) Photo documentation of any breaches flagged by the system are saved for management review. Teleperformance also uses this software for agents engaged in video customer interactions, to monitor agent position in front of the webcam and their compliance with work apparel rules.\(^{26}\)

AI tools have been adopted in workplace training and development programs, automating employee assessments, developing specialized training programs, and providing real-time feedback to employees.\(^{27}\) AI tools have also been adopted for automated, demand-driven scheduling.\(^{28}\)

In the 2022-23 Cornell/McMaster survey of CWA-represented call center workers, a majority of respondents reported the use of AI tools for automated monitoring and other management functions in their workplace. For example, the use of AI to automate monitoring of employees’ workspace was reported by 66% of survey respondents. The use of AI to give automated feedback on voice tone, pace, script adherence or call content were reported by 57% of survey respondents. Tools to automate the scheduling of hours and breaks were reported by 66% of survey respondents and tools that helped with training and development were reported by 64%.\(^{29}\)


\(^{25}\) Peter Walker, Call centre staff to be monitored via webcam for home-working ‘infractions’, The Guardian (Mar 26, 2021) [https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions

\(^{26}\) Deighton, supra n. 18


\(^{28}\) Lindsay Rose, Al-Powered Employee Scheduling: How Does It Work?, TSPSoftware.com (Nov 15, 2022) [https://humanity.tcpsoftware.com/blog/ai-powered-employee-scheduling-how-does-it-work.html

\(^{29}\) Data provided by Cornell University to Communications Workers of America (June 2023)
3. CWA call center members report that AI tools increase workplace stress, speed up the work, lead to more monitoring, and result in lower job satisfaction.

Respondents to the 2022-2023 Cornell/McMaster call center worker survey reported strongly negative reactions to automated monitoring tools in the workplace. Majorities of respondents reported negative opinions on the impact of AI tools that monitor the employees’ workspace and provide automated feedback, while small shares of respondents reported positive views. Regarding AI tools’ impact on stress levels in the workplace, respondents' views of tools used for monitoring were 67% negative, 24% neutral, 9% positive, with similar views on tools used for feedback (55% negative, 32% neutral, and 14% positive). Similar shares of respondents felt these tools do not make work more fair, easier, or interesting and do not improve customer service. Respondents reported slightly more positive views on the impact of AI automated feedback tools on customer service quality with 44% reporting negative views, 37% neutral and 19% positive.30

Survey respondents reported more mixed or neutral assessments about AI tools assisting with training and development and the scheduling of hours and breaks. Regarding automated scheduling tools, 40% said that they made work more stressful, 44% reported no opinion and 16% reported that they did not make work more stressful. Regarding automated training and development tools, 31% reported that they made work more stressful, 44% reported no opinion and 25% reported that they did not make work more stressful.31

The increased use of AI tools was correlated with work speed-up. The total aggregate time reported between calls each week was 108 minutes on average for those reporting no AI tools compared to 48 for those reporting the highest number of AI tools in use.32 The increased speed of work was similarly reflected in the survey respondents’ opinions of AI impacts. Seventy-seven percent of those using the most AI tools reported that they do not have enough time between calls, compared to 48% of workers who do not use AI tools.33 One call center member interviewed by CWA reported that automated call routing tools distribute calls at a relentless pace, even past the completion of work shifts:

So another thing that we have going on is that when you're in “after call work” [time between calls to finish paperwork or administrative duties], that won't stop calls from coming in, there are calls in queue... So you may not be done doing whatever you need to do when you have another call coming in... And like, if you’re finished, like, let's say your shift ends at 1:00 o'clock, then let's say it's 1:10 and then you're in “after call work”... it's gonna take you out of “after call work” and give you the next call even though your shift is over.34

The increased use of AI tools also enables greater frequency of monitoring, with 59% of the workers using the highest number of AI tools reporting that screenshots are taken often or

30 Cornell, supra n. 29
31 Cornell, supra n. 29
32 Cornell, supra n. 29
33 Cornell, supra n. 29
34 AT&T Mobility worker interview (June 2023)
constantly during the day and 76% reporting that their tone of voice and emotion were monitored often or constantly during the day. Workers using more AI tools were also more likely to agree or strongly agree that monitoring is used for discipline and reported higher discipline rates.\textsuperscript{35} One comment from the survey illustrates the pressure that arises from intense monitoring:

\begin{quote}
We are all under a microscope with managers looking at stats stats stats and expecting all of us to perform like robots. There are cameras everywhere, every second is documented, all key strokes are recorded, all calls are recorded. We are simultaneously told to be an advocate for the customers but then chastised or disciplined for doing just that.\textsuperscript{36}
\end{quote}

The number of AI tools was also correlated with greater reported amounts of customer abuse.\textsuperscript{37} CWA members interviews indicate that this may be a result of poor quality customer-facing technology (such as interactive voice response (IVR) systems using AI voice recognition and automated call routing) leaving customers frustrated:

\begin{quote}
There is a cause and effect if that AI cannot pick up an accent it will frustrate that customer to repeat over and over again what they're actually trying to call in for. When they actually get to a representative they're already in fumes by the time we're actually on the phone, which makes it harder to take that call and solve that customer's issue.\textsuperscript{38}
\end{quote}

AI tools were found to be correlated with higher absenteeism, high turnover intention and lower job satisfaction.\textsuperscript{39} However, the impact of specific AI tools on job satisfaction differed. AI tools used for monitoring had significant negative effects while AI tools that assist agents with finding product and customer information and AI tools associated with training and developing had a positive effect on job satisfaction.\textsuperscript{40} This indicates roles that new AI technology could play in supplementing and supporting a higher-skilled workforce of customer service professionals with higher job satisfaction.

\begin{itemize}
\item \textbf{a. Workers’ Describe the Limitations of AI “Sentiment Analysis” Monitoring Voice Tone, Conversation Pace, and Empathy Cues}
\end{itemize}

CWA members using CallMiner at Lumen Technologies report that the automatic assessment of emotions like empathy can be biased against workers of color and lack a nuanced analysis of customer interactions.

\begin{quote}
They are using a software called Call Miner. Black people have a tendency to be more direct, less soft in how we talk, but that doesn't mean we’re not being polite. I’m tired of hearing “you’re not hearing empathy”. I grew up military, I don’t know how to be a schmoozer, that’s never been instilled in me. I’m half German half Black, you say it how it
\end{quote}

\textsuperscript{35} Cornell, supra n. 29
\textsuperscript{36} CWA/Cornell 2023 Survey Comment
\textsuperscript{37} Cornell, supra n. 29
\textsuperscript{38} AT&T Mobility worker interview (June 2023)
\textsuperscript{39} Cornell, supra n. 29
\textsuperscript{40} Cornell, supra n. 29
is. People want to get on and off the phone. That’s not good enough for Call Miner. You can’t judge a call by phone with a computer system.\textsuperscript{41}

Similar concerns have been raised about CallMiner at Santander Bank, where the CallMiner analysis has been used for evaluation and compensation decisions.\textsuperscript{42}

In addition to concern around bias, the CallMiner automated analysis system enables managers to circumvent union contract language which limits the number of calls managers may observe and requires that calls be randomly selected for evaluation. In focus groups, CWA members explained that CallMiner’s visual dashboard flags calls for review, which allows managers to cherry-pick which calls to evaluate for an agent who is disfavored, and to initiate disciplinary action more easily.

I know with my folks I deal with on-going issues regarding the AI system, if that’s what you guys call it, which tracks the tone of the voices between the customer and the agent where it boiled down to where the employee felt like they were being racially profiled or that they feel like their gender was being questioned. So we deal with that... We just have to deal with those issues as they come. A lot of them is when the employee’s being investigated for customer abuse. Or it could be that they didn’t make their numbers for that month. And so the manager will go in and cherry pick and instead of actually listening to a call they’ll pull up that system and see which call had high reds or greens or show the different flow of the call and they’ll say “oh okay I’ll pick that one and ob[serve] that one this month or ob[serve] that and then that employee ends up being disciplined for it. So that’s kind of what my folks are going through.\textsuperscript{43}

Front-line employees are often not fully aware of the level of surveillance they are under, and only become aware when they are disciplined. Union representation in disciplinary meetings ensures that there is a process for human intervention. Otherwise, discipline and dismissal decisions may be made solely on the basis of automated AI analysis.

Normally they [workers] don’t find out unless they’re being reprimanded... They [managers] don’t specifically say “we are recording every piece of your conversation and from each keystroke.” Of course they covered us and say it could be used for developmental purposes and you’ll get dealt with if it’s on an egregious level. But a lot of my folks don’t find out until they’re pulled into the room. At that point I’m privy to the information and that’s when we start dissecting it. Like, “okay, well you got this ding from the observation department, but did you really take a look and actually go in to listen to the call before you decided to pull them offline and reprimand them?” Well now we’re listening to the call, just because it showed red it was not because it was a “gross customer service abuse” moment, it was more of this particular situation. And so

\textsuperscript{41} Lumen employee interview (August 2022)
\textsuperscript{43} Lumen employee interview (May 2023)
oftentimes the employee goes through the distress with no findings and/or there is finding but we’re picking it apart as far as the intent at this point. So it just depends. On the average basis, I don’t have a member that comes up to me and says “I feel uncomfortable because the algorithm or the AI system is capturing this data,” until they’re actually in trouble or something.44

CWA call center members at Verizon report the use of a software called Cogito. While workers are concerned about potential use for discipline, management has so far not used the system as the basis for discipline. Local leadership report that the long-seniority, highly experienced membership there gets little value from the prompts generated by Cogito.

Here’s my opinion on it. The reason it’s not a big deal is that we’re not a cheaply run, high turnover call center, where the average employee lasts 90 days. I’ve been here 11 years plus. Some of the other people taking these calls have been here 20, 30 years. So you’re dealing with people who are pros at this. I think it might be more helpful in a situation where you’ve got untrained people doing these calls with a high turnover rate to make them better on the phone. It doesn’t seem to fit the level of knowledge we have.45

This assessment is in line with the outcome of a recent study of generative AI tools used by customer support agents, which found that their greatest impact on productivity was among less-experienced, lower-skilled workers, with minimal improvements for experienced and highly skilled workers.46

At unrepresented call centers using Cogito, workers have expressed frustration that Cogito’s analysis is often confused, interpreting any tonal variation, such as laughter, as emotional distress and overly rigid, requiring agents to continually repeat “sorry” to meet empathy metrics.47

Non-union workers at major federal government contractor Maximus are monitored by AI systems that depict call evaluations as graphics, allowing managers “to monitor several agents’ calls at the same time and spot changes in mood or long periods of silence.”48 According to a Maximus executive, this represents an expansion of management oversight. Previously, “quality managers used to listen to two calls per agent per week.”49 Maximus workers have engaged in multiple strikes in 2022 and 2023, over a number of issues, including to protest a high stress, tightly managed environment governed by automated call-flow software, and made worse by inadequate bathroom breaks and insufficient time between calls to catch their breath and handle administrative matters.50

---

44 Lumen employee interview (May 2023)
45 Verizon employee interview (September 2022)
48 Deighton, supra n. 18
49 Deighton, supra n. 18
50 Sophie Putka, Workers Strike at Medicare, ACA Call Centers, MEDPAGE TODAY (Aug. 9, 2022),
b. Workers’ Report Harms from AI Technology Used for Script Adherence

CWA call center members at AT&T Mobility reported increased stress from constant monitoring and real-time script adherence enforcement using HiPer. Strict script adherence eliminates agent discretion, making it more difficult to resolve customer issues.

I can see in the workplace new technologies coming on line to increase pressure and control. New software called HiPer has, just this month, been introduced to our workflow. This software monitors our call in real time to check that important key words associated with our sales script are used. The software requires us to stick to scripts that don’t always relate to the situation on our calls or what the customer needs. I’m a human but I am increasingly treated like a robot. New technology, like HiPer, dramatically expands the ability of managers to automatically and constantly surveil all work performed.  

AT&T’s use of automated tools to enforce sales requirements creates a stressful work environment for agents and may harm customer service.

All of these tools are often used to drive an unrelenting push for sales. Every customer that calls, for any reason, must be pitched to buy new services. And these sales pitches cannot be brief “fly by” pitches. We are supposed to probe every customer with questions about their family, occupation, and even travel plans to make personalized sales offers for them. This pressure to sell and the various ways that managers can monitor me creates an enormous amount of stress. Over the past few years in this position, the stress has made me sick to my stomach and unable to get out of bed in the morning to do my job. I’ve started taking FMLA time as a result of missing work days due to stress. I know my experience is not unique. I’ve heard from many co-workers that are having similar issues.

CWA agents report that the analysis and guidance generated by HiPer is often confused and can contradict company policies, creating a situation where agents can be disciplined as a result of following the automated guidance from HiPer.

HiPer is designed to guide the representative throughout the call on what they should say to the customer. The system captures key phrases and makes suggestions to the representative on what they should do next. However, the system often gets confused, is unable to help solve problems, advises the wrong solution, and lags indefinitely. This makes HiPer feel like more of a distraction than a helpful tool.

51 AT&T Mobility worker interview (Feb 2023)
52 AT&T Mobility worker interview (Feb 2023)
Additionally, HiPer often guides us to do things that conflict with company policies and procedures. For example, if a customer requests a cancellation for their tablet, HiPer will prompt you to offer customers new promotions and services. This offer goes against company policy because you can’t cancel a line and add a new line on the same call. The company calls this a “flipper.” Representatives can be penalized with a “Code of Business Conduct” violation for flipping even when HiPer is instructing them to do this. A violation like this could go as far as termination for the worker. In fact, there have been times where representatives got in trouble for this, but thanks to our union, we were able to work with the manager to do coaching instead.

This is all so frustrating because I know my job well, I understand the needs of my customers, and I have great customer service. But, when I’m forced to use this tool, I’m not able to be as effective and my scores suffer. AT&T has a report to see if the representative is using HiPer. Honestly, I’m worried that this could end up jeopardizing my incentive pay.

Similar to the “sentiment analysis” monitoring tools reviewed above, automated script-adherence tools are being used by managers to circumvent limits on monitoring observations under the collective bargaining agreements. Call monitoring observations are intended to be random, but managers now have the ability to use visual dashboards and automated AI analysis to cherry pick calls flagged by the system:

[B]ased on our contract, the maximum amount of calls supposed to be monitored is eight. And it [the union contract] specifically says randomly picked calls. And the AI is tracking everything, you know, transcribing everything. So now the manager can go in and, not go into the normal system, to take a look and kind of take a peek at which one they want to pull first... When we negotiated that, we wanted it to be a random pick by the manager first, then the next call would be picked by the rep, then the next call picked by the manager and since AI has come in that's all, you know, it's very, very hard for us to enforce that.


As new technologies have been implemented in call centers over time, CWA members have bargained for contract language that protects workers. These provisions remain critical in the face of new AI technologies discussed here. CWA contracts include language that requires prior notification of monitoring sessions, reduces the amount of monitoring, and requires that monitoring be used for coaching and development, not discipline. CWA contracts protect against the speed-up enabled by new technologies by guaranteeing time between calls to resolve complex customer issues and handle administrative work. New work-from-home agreements

53 Statement by CWA Member Ylonda Sherrod (Jun 1, 2023)
54 AT&T Mobility worker interview (June 2023)
55 CWA Customer Service Issue Briefs supra n. 17
bargained by CWA units limit web camera surveillance of agents’ work areas, so that video is used only for coaching and clean desk inspections. These agreements also require advance notice before web cameras will be used. These contract protections are critical to preserving job quality for CWA call center members and illustrate the importance of union representation and collective bargaining to protect workers’ interests in the midst of rapidly changing workplace technologies.

Governmental policy can play a critical role in providing institutional support for workers’ collective bargaining rights, for instance by strengthening penalties for employer violations of labor law and requiring just cause for terminating employment. To address automated surveillance and management technologies in particular, the NLRB General Counsel has identified the need to preserve workers’ rights to organize and bargain by establishing a new framework of enforcement that recognizes the chilling effect these technologies can have on protected concerted activity. Employers should be required to bargain in good faith with their employees’ unions over the adoption and impact of automated workplace surveillance and management technologies, which qualify as mandatory subjects of bargaining under the National Labor Relations Act.

AI technologies also require new regulatory frameworks to protect workers and the public. Coordinated federal action is required to enshrine in law the principles articulated in the Administration’s “Blueprint for an AI Bill of Rights.” This should include steps recently advocated by CWA in comments to the Federal Trade Commission: (1) requiring meaningful transparency from employers when automated management systems are used for critical worker management functions such as recruitment, performance evaluation and management, work allocation and dismissals, (2) prohibiting automated management practices if they may tend to discriminate on the basis of race, age, gender, ability and other protected characteristics, (3) requiring meaningful human oversight of automated management system that may result in termination, and (4) establishing procedural standards such that those affected by algorithmic decisions have real opportunities to have mistakes reversed and similar recourse.

---

56 2022 Regional Labor Agreement between the Communications Workers of America and AT&T Mobility Services LLC, Memorandum of Agreement Work from Home (WFH) at 86 https://cwa-union.org/sites/default/files/att_mobility_orange_contract.pdf; 2022 Common Issues Memorandum of Understanding Between Verizon New York Inc… and Communications Workers of America, AFL-CIO, Attachment 3 Work-At-Home Memorandum of Agreement at 20
60 Communications Workers of America, Service Employees International Union, Strategic Organizing Center, COMMENT TO THE FEDERAL TRADE COMMISSION Re: Advanced Notice of Proposed Rulemaking Regarding Commercial Surveillance and Data Security, Docket # FTC-2022-0053 (November 21, 2022)
This should also include safeguards to protect worker data privacy, by requiring employers and third-party vendors contracted by employers to follow data minimization principles that limit data collection to the data elements that are directly relevant, that are necessary for a legal purpose, and maintain data for limited time. Worker consent should also be required before employers or third-party vendors share, sell, aggregate, process, or transfer data or information collected about an employee.

We look forward to continued engagement with the OSTP and federal agencies as these important issues are further reviewed and addressed.
The Action Center on Race & the Economy (ACRE) writes in response to the request for information regarding automated worker surveillance and management.

Attachments

ACRE OSTP Comment Letter
To Whom It May Concern:

The Action Center on Race & the Economy (ACRE) writes in response to the request for information regarding automated worker surveillance and management. ACRE drives campaigns that fight for racial and economic justice and challenge the institutions responsible for pillaging communities of color and poor families and destroying our environment. As a part of our work, we support groups organizing app-based workers working to address the compounding health, safety, and wage crises perpetuated by app corporations like Uber, Lyft, and DoorDash.

This comment draws from existing research and analysis on the harms of worker surveillance and automated management on app workers, particularly app workers of color. Moreover, the comment relies on challenging the foundational problem at the core of app work: the business model of corporations like Uber, Lyft, and DoorDash automate perpetual economic precarity and push workers into unsafe situations without essential workplace protections.

The App-Based Industry’s Capture & Exploitation of Workers of Color

Uber and Lyft emerged from the economic ashes of the global financial crisis in 2008. In a few short years, Uber, Lyft, and other app-based corporations became ubiquitous, with drivers and delivery workers in all 50 states. Researchers have highlighted that far from serving as a “fix” to the financial crisis, these corporations used widespread economic distress to organize vast numbers of unemployed workers, primarily people of color and immigrants, into a cheap, disposable workforce. App work like driving for Uber and Lyft is not new—it is a re-creation of decades-old business practices which rely on Black, Brown, and immigrant labor to offload costs.

---

2 In this document “app-based corporations” describes Uber, Lyft, and other businesses such as DoorDash and Grubhub, which pay workers a per-job amount instead of a wage to provide an on-demand product or service.
onto workers, cut corporate expenses, and carve these workers out of basic workplace protections.⁴

This trend continues today. In the corporation’s Q4 2022 investor call, Uber mentioned that inflationary pressure allows the corporation’s supply of drivers to thrive.⁵ More workers join Uber’s platform in a recession—and given Uber’s model, they are trapped in precarious, unsafe work with unpredictable pay and little to no benefits. Research shows that inflationary pressures and economic recessions most impact Black and Brown workers—corporations like Uber capture vulnerable workers through the rhetoric of flexibility and agency. Yet the app is automated, and workers are directed by an unaccountable boss.

### The Automated Surveillance & Management Behind App Work

#### Data Collection & Algorithmic Decision-Making from Onboarding to Termination

When Uber and Lyft drivers log on to the app, they are subjected to constant digital surveillance. Drivers are expected to provide their own cell phone and car, install the app on their personal devices, and submit to intensive identification and background checks.⁷ This allows Uber and Lyft to engage in intrusive surveillance and data extraction. App-based drivers have reported location tracking notifications while their apps were closed, high battery consumption, unusually high levels of data usage after giving the app permission to access their phone’s storage, and receiving notifications suggesting they log in while using a competing platform.⁸

Once the app is installed, facial recognition technology in the phone camera monitors driver identification requirements.⁹ The app tracks drivers’ GPS location, speed, acceleration, and hard stops.¹⁰ It monitors drivers’ acceptance, cancellation, and completion of passenger ride requests.¹¹ It records driver and passenger in-app communications, as well as passengers’ ratings of each driver after the ride.¹² The app instructs drivers which passengers to pick up where, what the driver’s estimated time of arrival is, and what directions a driver should follow to

---


⁵ *Uber Technologies (UBER) Q4 2022 Earnings Call Transcript*, Fool (Feb. 8, 2023), [https://tinyurl.com/mr246yf5](https://tinyurl.com/mr246yf5).


⁸ S. Sannon, supra n. 7, p. 6.

⁹ *Why Am I Being Asked to Take a Photo of Myself?* Uber, [https://tinyurl.com/4jpxbd7](https://tinyurl.com/4jpxbd7) (last visited Jun. 8, 2023); Biometric Information and Security Policy, Lyft (Sept. 8, 2021), [https://tinyurl.com/46vb943y](https://tinyurl.com/46vb943y).


¹² Uber Privacy Notice, supra, n. 10; Lyft Privacy Policy, supra, n. 10.
a passenger’s destination. If drivers deviate from these instructions, they risk discipline or, depending on the circumstances, even “deactivation” from the app.

Data from the app’s meticulous tracking of every aspect of the driver’s work is fed into an algorithm that makes the kind of decisions normally made by a human supervisor. The app determines which rides to allocate to which drivers and how much to compensate drivers for those rides. Extracted data also continuously fine-tunes predictions about drivers’ future behaviors, which the app then uses to create individualized, gamified bonuses and other financial incentives to encourage workers to keep driving on the app’s desired terms. The algorithm uses this data, including passengers’ reviews, to evaluate drivers. Sudden suspensions or deactivations from the app via electronic notification are not uncommon, and terminating drivers is highly dependent on data gathered through electronic surveillance.

**Algorithmic Wage Discrimination**

Automated worker surveillance and management systems can produce outcomes that result in unlawful discrimination when they function as “black boxes” with internal workings not clear to most people, including, in some cases, even the developer of the tool. The “black boxes” at the center of other app-based corporations’ automated systems are the algorithms they use to allocate rides to drivers and to determine driver compensation. These automated pay algorithms allocate individualized, temporary financial bonuses to drivers, which many drivers view as essential to supplement their otherwise inadequate earnings. These algorithms, which personalize wages based on driver data, are proprietary and, thus, unknowable to drivers. In a phenomenon legal scholar Dubal has described as “algorithmic wage discrimination,” the apps create a system in which drivers doing the same work, with the same skill, for the same company, at the same time, may earn very different hourly pay.

As Dubal explains, the large amounts of data on driver behavior at app-based corporations’ disposal, along with their growing technological sophistication, create the ever-increasing possibility that their algorithms can “calculate the exact wage rates necessary to incentivize

---

14 In this document, “deactivation” refers to when an app-based company blocks a worker’s access to the app either temporarily or permanently too often without warning or just cause. Essentially, deactivations are terminations or unpaid suspensions.
16 E. Vignola et al, *supra* n. 11, p. 4; A. Mateescu et al., *supra* n. 13, p. 5-6.
17 Ibid.
21 E. Vignola et al., *supra* n. 11, p. 4.
desired behaviors.” Thus, “algorithmic wage discrimination allows firms to personalize and differentiate wages for workers in ways unknown to them, paying them to behave in ways that the firm desires, perhaps [paying] as little as the system determines that they may be willing to accept.” Dubal describes examples of drivers being forced to wait for 45 minutes in a busy area to get dispatched the final ride to qualify for a $100 bonus, or being subjected to a kind of “casino mechanics” in which the hope of being dispatched a lucrative ride keeps drivers on the road for longer.

Furthermore, at least one of Uber’s issued patents indicate that algorithmic wage discrimination is likely a part of the corporation’s business model based on many data points about drivers. A patent issued in May 2023 for “computing estimated value of providing service among geographical regions” is pitched as a tool for drivers to predict how much they may earn on any given day. Uber mentions that the data points fed into the tool may also be used to determine the likelihood of driver behavior. In other words, this data that the company almost certainly collects, and is at least considering collecting, may be used to determine driver fares.

The patent notes that this information, in the form of a “user profile,” may include the “type of service provided, provider ratings, data about past service, an average number of services provided per hour, vehicle type, common hours online, an average arrival time in relation to a predicted estimated time of arrival, whether the provider typically follows suggested service instructions (e.g., routes), geographical regions most frequently visited by the provider, an average amount of time the provider is willing to wait for a new assignment,” and more.

Data points such as “average amount of time the provider is willing to wait for a new assignment” are indisputably predatory, automating decision-making about wages on the basis of driver desperation.

Dubal points out that “even if on-demand companies are not using algorithmic wage discrimination to offer vulnerable workers lower wages based on their willingness to accept work at lower prices, the possibility remains that they can do so.” Even more alarmingly, due to their systems’ opacity and increasing complexity, there is no real way for workers, the public, or in some instances, even regulators, to verify that they are not doing so. Some qualitative research already documents app-based drivers’ anecdotal experiences that as they drive more on the platforms—and thereby signal greater economic desperation—they receive fewer financial incentives.

As more data on drivers’ activities both inside and outside of work is collected and sold among corporations, a scenario becomes increasingly plausible in which app-based corporations could

23 Id., p. 6.
24 Ibid.
25 Id., p. 36.
26 Id., p. 40.
28 Ibid.
29 V. Dubal, supra n. 22, p. 40.
30 A. Zhang et al., Algorithmic Management Reimagined for Workers and By Workers, CHI Conference on Human Factors in Computing Systems, New Orleans, LA (Apr. 2022), https://tinyurl.com/ms64fse7 (noting “Drivers unanimously agreed that Quest [bonus] offers were determined by the frequency of driving, drawing from personal and other driver experiences: the more a driver worked, the worse the bonus offers they would receive.”)
feed outside data, such as credit card debt or court judgments, into their algorithms to pin-point which workers are the most financially desperate, and thus the most likely to accept the lowest compensation.31 App-based companies already partner with financial services institutions to offer drivers bank accounts and credit and debit cards.32

Most app-based workers are people of color and immigrants,33 and this is no coincidence. History has shown us that corporations and other financial institutions target Black and Brown workers, particularly those in economic desperation, through their predatory products and business models.34 Uber and other app-based corporations’ practices are no exception and a continuation of the technology and financial industries targeting people of color for market control and higher profits.

By engaging in algorithmic wage discrimination, Uber’s and Lyft’s platforms upend deeply rooted principles of equal pay for equal work and of the fairness and predictability of wages, hurting workers of color most.35

The Harms of App Work’s Automated Surveillance & Management

Workers’ Pay, Benefits, and Employment

Uber and app-based corporations like Lyft that adopted a similar business model are some of the most prominent examples of how automated worker surveillance and management systems can erode drivers’ capacity to earn a decent living.36 A key strategy Uber used to gain early market dominance was to get passengers to expect an “on-demand” ride.37 Uber achieved this by adopting technology so that virtually anyone with a car could work on their app, thus flooding the market with drivers and exerting tremendous downward pressure on drivers’ wages.38

Uber and Lyft have used their algorithms to push drivers’ wages so low that it’s nearly impossible for drivers to make enough even to support one person, let alone a family.39 According to a nationwide study published in 2022, nearly two-thirds of gig workers nationwide earn less than $15 per hour, and 29% earn less than the minimum wage in their state.40 Similarly, a 2022 study in Denver found that drivers for Uber, Lyft, and DoorDash take home

37 Ibid.
38 Ibid.
only $5.49 per hour after expenses, working in a city with a minimum wage of $15.87. A 2022 California study found that Uber and Lyft drivers take home an average of only $6.20 per hour after subtracting expenses and the cost of key benefits not afforded to drivers.

Further exacerbating their financial insecurity, drivers may be deactivated by the app unpredictably and for seemingly arbitrary and opaque reasons. A 2023 survey of over 800 California drivers found that two-thirds of those surveyed had been deactivated temporarily or permanently. A national survey of over 900 drivers found that 40% of respondents had been deactivated in the last year. Thirty percent of drivers reported the companies failed to provide any explanation for their deactivation.

For drivers, the consequences of deactivation can be severe. Nearly one in four deactivated drivers responding to the 2023 California survey reported difficulty paying for schooling, childcare, or other child-related expenses. In the same survey, more than one-quarter of deactivated drivers (28%) experienced difficulty paying medical insurance, medical bills, and costs. Eighteen percent of drivers reported losing their car after deactivation; devastatingly, as many as 12% of deactivated drivers reported losing their home.

**Workers’ Physical and Mental Health.**

The health and safety crisis among app-based drivers is no accident. Relying on a business model that pays low wages and that shifts responsibility for occupational safety to drivers, Uber and Lyft have created some of the most dangerous jobs in the nation.

Researchers have coined the term “algorithmic insecurity” to describe the continuous worry and fear that app-based workers experience about their ability to access work, decent pay, and reasonable working conditions when laboring in an unstable and opaque online environment. The need to work consistently and accept jobs as they become available aggravates stress, as does the financial pressure to overwork or to work irregular hours, which can lead to anger.

---

41 E. Leverage, supra, n. 39, p. 5.
43 U.S. Terms of Use, Uber (Jan. 17, 2023), Termination, §1 (reserving right to “terminate these Terms or any Services with respect to you … at any time for any reason”), https://tinyurl.com/2p9zh8bh; Lyft Terms of Service, Lyft (Dec. 12, 2022), Termination, §16 (reserving right to immediately deactivate if “you fall below Lyft’s star rating or cancellation threshold”), https://www.lyft.com/terms.
46 Fired by an App, supra, n. 44, p. 4.
47 Id., p. 18.
48 Ibid.
49 Ibid.
50 P. Leigh, Open Forum: Driving for Uber, Lyft, GrubHub and others is one of the most dangerous jobs in the country, San Francisco Chronicle (Jul. 25, 2019), https://tinyurl.com/mrybezr.
depressive symptoms, poor sleep, and exhaustion.\textsuperscript{52} Researchers have also observed that the platforms’ so-called ‘gamification’ techniques of unpredictably eliciting drivers to accept consecutive challenges to unlock financial rewards resemble techniques to promote compulsive gambling.\textsuperscript{53} The constant surveillance and management of workers through the app substitutes interpersonal explanation for an automated decision, leaving many drivers feeling ignored and isolated, with negative mental health consequences.\textsuperscript{54}

App-based work is also physically dangerous. According to a 2023 survey of over 900 Uber and Lyft drivers nationwide, two-thirds of all rideshare drivers reported being threatened, harassed, or assaulted in the last year.\textsuperscript{55} A majority of driver respondents reported being verbally abused;\textsuperscript{56} more than a quarter reported being verbally threatened with physical harm, and more than 14\% reported being grabbed, groped, or hit.\textsuperscript{57}

Even worse, the combination of Uber’s and Lyft’s algorithmic systems of low pay and frequent and seemingly arbitrary deactivations strongly incentivize drivers to drive passengers who appear too drunk to transport safely, are behaving unpredictably, or are requesting a ride that feels like a set-up for a potential robbery or assault. The same 2023 national survey found that the most common reason for accepting a ride that made drivers feel unsafe—cited by 59\% of drivers—was fear that passengers might leave negative reviews leading to deactivation.\textsuperscript{58} Another 49\% of drivers reported accepting unsafe rides out of fear that their cancellation rates would rise above acceptable levels, and another 43\% reported accepting unsafe rides out of fear their acceptance rates would fall too low.\textsuperscript{59} More than half (57\%) of drivers also reported accepting unsafe rides because they feared losing income.\textsuperscript{60}

The stakes of this health and safety crisis could not be higher. A review of press reports, police reports, and court records reveals that in 2022 alone, at least 31 app-based drivers and delivery workers were murdered on the job.\textsuperscript{61} Similar research found that over 50 drivers were killed on the job between 2017 to early 2022, bringing the total to at least 80 drivers that were murdered between 2017 to 2022.\textsuperscript{62} The true numbers may be higher, as these numbers are based on the public record alone, and in nearly every state, app-based corporations are not required to report instances of violence, assault, workplace injury, or homicides to government agencies.\textsuperscript{63} Even
so, if the United States Bureau of Labor Statistics treated app-based work as a sector, it would likely be among the top five sectors where workers are killed on the job.\textsuperscript{64}

\textit{Workers’ Ability to Exercise Workplace Rights}

Automated workplace management and surveillance tools also impact drivers’ ability to exercise their rights collectively. Even accounting for gig workers’ higher levels of financial strain, researchers report increased powerlessness and loneliness among app-based workers, concluding that algorithmic control and distancing strategies may undermine worker autonomy and meaningful connection\textsuperscript{65}—which can play a key role in building collective demands.

When drivers raise their collective concerns, this same social and spatial isolation can also make it more difficult for workers to have their voices heard. As legal scholar Brishen Rogers highlights, app-based workers currently do not have the right to use their employer’s website, app, or other technological platforms to communicate with the public.\textsuperscript{66} As Rogers explains, “There simply is no digital equivalent to the in-person picket line or leafleting effort on or near the employer’s physical property.”\textsuperscript{67} Brishen directly contrasts drivers’ lack of access to such a space with the out-sized power of app-based companies to use that same digital space as a megaphone for their ends. Uber and Lyft inundated drivers and passengers with in-app messages to support Proposition 22, a 2020 California ballot initiative that reduced drivers’ employment rights.\textsuperscript{68} This spring, Uber emailed Minnesota drivers and passengers with links to state lawmakers urging them to oppose a drivers’ rights bill.\textsuperscript{69}

As data surveillance technologies become more cheap and ubiquitous, app-based corporations will be increasingly capable of building large, aggregated data profiles that allow them to screen for nascent organizing efforts or for workers more likely to participate in collective action.\textsuperscript{70} This reality may not be far off. Uber already receives geofence warrant requests, which can use smartphone data to collect the identities of people at protests and other large-scale political events.\textsuperscript{71} Conceivably, companies could use such data to screen out prospective workers they deem unlikely to defer to management authority.\textsuperscript{72} As Rogers highlights, under current law, workers and even regulators may struggle to identify or access the underlying surveillance algorithms to even determine if such practices are occurring.\textsuperscript{73}

\textit{App-Based Algorithmic Management & Technologies Hurt Workers of Color Most}

\begin{flushleft}
\textsuperscript{64} Ibid.
\textsuperscript{65} P. Glavin et al., \textit{Uber-Alienated}, Work and Occupations, 48(4) (Nov. 2021), \url{https://tinyurl.com/vckvemj}.
\textsuperscript{66} B. Rogers, \textit{supra}, n. 36, p. 95.
\textsuperscript{67} Ibid.
\textsuperscript{68} Ibid. See also K. Lyons, \textit{Uber accused in lawsuit of bullying drivers in its app to support Prop 22}, The Verge (Oct. 22, 2020), \url{https://tinyurl.com/5878ftb2}.
\textsuperscript{69} M. Nesterak, \textit{Uber warns customers and drivers}, Minnesota Reformer (May 16, 2023), \url{https://tinyurl.com/98puf}.
\textsuperscript{70} B. Rogers, \textit{supra}, n. 36, p. 99.
\textsuperscript{71} M. Guariglia, \textit{Geofence Warrants Threaten Civil Liberties and Free Speech Rights in Kenosha and Nationwide} (Sept. 10, 2021), \url{https://tinyurl.com/3danwff5}.
\textsuperscript{72} B. Rogers, \textit{supra}, n. 36, p. 97.
\textsuperscript{73} Id., p. 98.
\end{flushleft}
The big data algorithms used by Uber, Lyft, and other app-based corporations both preserve and amplify the deep racial and gender inequalities that pervade the present while also magnifying the power of corporations over workers. This Section addresses four aspects of such automated surveillance and management systems: (1) facial recognition technologies, (2) passenger reviews of drivers, (3) driver health and safety, (4) driver deactivations. As legal scholar Ifeyoma Ajunwa warns, “Governmental action is necessary to ensure that the future of work is not a dystopia for all workers, but especially for more vulnerable workers of color.”

**Facial Recognition Technologies**

From the instant app-based drivers log on to the app, Uber and Lyft use automated algorithms and facial recognition technologies to verify drivers’ identities, despite this technology being notoriously inaccurate for non-white and non-male faces. If the automated system fails to recognize the driver’s face, the driver can be locked out of the app and may be deactivated. In recent years, drivers of color in the United States and the United Kingdom have brought legal action against Uber, alleging racial discrimination because the app failed to recognize their faces and prevented them from working. A 2021 *Los Angeles Times* investigation similarly found that some transgender Uber drivers were deactivated after the app deemed their post-transition profile photos to be “fraudulent.”

Facial recognition technology is also deeply integrated into policing in the United States. Biometric data collection by Uber and other app-based corporations may lead to further harm to workers of color and immigrants who are at higher risk of police and law enforcement interaction and abuse. While the data-sharing relationships between Uber and law enforcement are unclear, more data collection could mean a higher risk for sharing with law enforcement actors and data privacy abuses.

---

81 The details regarding Uber’s data sharing relationships with police are unclear, but Uber’s law enforcement report indicates thousands of requests that the platform receives for data on riders and drivers. The total number of requests between 2019 to 2022 increased, indicating a higher reliance by law enforcement on Uber’s data. See *Transparency Report, Law Enforcement Requests*, Uber (last accessed Jun. 20, 2023), https://tinyurl.com/mscj6vmmn.
Furthermore, facial recognition technologies are also employed or considered by many other governmental actors: from federal agencies that provide social services to state employment agencies to local housing authorities. While there is no public evidence to suggest that Uber’s collection of biometric data feeds into these systems, it is not implausible that as Big Data and Big Tech further integrate into the provision of essential social services, workers of color who are most likely to depend on these services will be subject to a deeper, more intrusive surveillance net that Uber’s data capture may embolden.

Passenger Reviews of Drivers

Despite mounting evidence of racist outcomes, Uber, Lyft, and other app-based platforms rely heavily on systems in which passengers are asked to rate drivers after each ride in order to monitor and discipline drivers. Uber and Lyft drivers who receive insufficiently high passenger ratings are at risk for deactivation. Black and Brown app-based drivers report receiving lower ratings from passengers than white drivers, opening up what some researchers have described as a backdoor to discrimination.

This problem is long-standing. A 2016 study by Data & Society documents how Uber and other app-based corporations’ reliance on potentially biased passenger ratings may lead to a disparate impact on workplace outcomes. Legal scholar Richard Ford has described how such bias may be particularly pernicious in the context of algorithmic management because the numeric rating gives the illusion of data-driven objectivity while stripping the interpersonal evaluation that undergirds the rating of its social context. This both makes it easier for customers to hurt workers and harder for workers to prove discrimination.

Examples of passenger racism against drivers are all too frequent. In a national survey of over 900 app-based drivers, 39% of drivers of color reported being called a racial, ethnic, or religious slur by passengers. In a California survey of more than 800 current and former Uber and Lyft drivers, 50% of drivers reported experiencing bias or discrimination from passengers based on their race or national origin; and of those drivers, 50% reported that the passenger had filed a complaint against them with Uber or Lyft.

83 Lyft Terms of Service, supra n. 43 (reserving right to immediately deactivate if “you fall below Lyft’s star rating”), https://www.lyft.com/terms; Uber Community Guidelines, Uber (Oct. 20, 2021) (stating that “drivers … that don’t meet the minimum average rating for their city may lose access to all or part of the Uber Marketplace Platform”), https://tinyurl.com/3nz5f9hw.
86 Ibid.
87 S. Harnett, supra, n. 84.
88 Ibid.
89 Driving Danger, supra, n. 45, p. 9.
90 Fired by an App, supra, n. 44, p. 4.
Given the weight Uber’s and Lyft’s algorithms give to racist customer reviews and complaints, it is shocking but not surprising that drivers of color report being disproportionately deactivated. A study by Asian American Advancing Justice—Asian Law Caucus and Rideshare Drivers United found that drivers of color were significantly more likely than white drivers to have their accounts deactivated after passenger complaints.\textsuperscript{91} Of the 810 drivers surveyed, \textbf{69\% of drivers of color reported experiencing either permanent or temporary deactivation}, in comparison with 57\% of white drivers.\textsuperscript{92} Forty-two percent of deactivated drivers were told their deactivations were due to customer complaints.\textsuperscript{93}

\textit{Driver Health & Safety.}

The endemic violence directed towards app-based drivers has generated a racialized safety crisis. \textbf{According to a 2023 national survey, app-based drivers of color experience violence, harassment, and threats from passengers at higher rates than white drivers.}\textsuperscript{94} Sixty percent more drivers of color reported being robbed or carjacked in the last year compared to white drivers.\textsuperscript{95} Drivers of color were also 86\% more likely than white drivers to report being called a racial, ethnic or religious name or slur.\textsuperscript{96} One in five drivers of color report being physically grabbed, groped or hit, which is 37\% more than white drivers.\textsuperscript{97} Drivers of color also report being verbally threatened with physical harm 24\% more than white drivers and are three times more likely than white drivers to have been shot or stabbed in the last year.\textsuperscript{98} \textbf{Of the 31 app-based drivers researchers identified as murdered on the job in 2022, 77\% were people of color.}\textsuperscript{99}

App-based drivers also experience high rates of sexual harassment and assault while working on the platform. In a 2023 survey of California drivers, 43\% of drivers reported experiencing sexual harassment on the job (53\% of female drivers, 41\% of male drivers).\textsuperscript{100} In a 2023 national survey, 27\% of drivers reported being sexually propositioned, 14\% reported being physically grabbed, groped, or hit, and 3\% reported being sexually assaulted or raped.\textsuperscript{101}

The alarming rates of violence that app-based drivers of color experience are rooted in Uber’s and Lyft’s algorithmic management systems. Because of the higher rates of bias, they face from customers,\textsuperscript{102} drivers of color are acutely aware that if they cancel a ride with a threatening passenger and later receive a negative review or complaint, they may be summarily deactivated.\textsuperscript{103} In the 2023 national survey, a higher percentage of drivers of color—64\% as

\begin{flushleft}
\textsuperscript{91} Ibid.
\textsuperscript{92} Ibid.
\textsuperscript{93} Ibid.
\textsuperscript{94} \textit{Driving Danger}, supra, n. 45, p. 9.
\textsuperscript{95} Id., 10.
\textsuperscript{96} Ibid.
\textsuperscript{97} Ibid.
\textsuperscript{98} Ibid.
\textsuperscript{99} \textit{Murdered Behind the Wheel}, supra, n. 61, p. 5.
\textsuperscript{100} \textit{Fired by an App}, supra n. 44, p. 4.
\textsuperscript{101} \textit{Driving Danger}, supra, n. 45, p. 7.
\textsuperscript{102} See n. 84-94, supra, and accompanying text.
\textsuperscript{103} \textit{Driving Danger}, supra, n. 45, p. 12.
\end{flushleft}
compared to 55% of white drivers—reported providing rides to threatening passengers. Drivers of color were also 30% more likely than white drivers (74% vs. 54%) to report having provided a ride to a passenger in the last year who made them feel unsafe due to concerns that the passenger might leave negative reviews. Drivers’ documented experiences demonstrate how the disparate impacts of Uber’s and Lyft’s automated management systems push drivers of color into situations where they face a heightened risk of being victimized by passengers.

**Deactivations**

One of the most salient features of the automated surveillance and management systems of Uber, Lyft, and other app-based corporations, is just how swiftly and frequently drivers can be deactivated—at times, seemingly based on passenger whims—while, in contrast, passengers generally face much less intensive discipline. As journalist, researcher, and activist Dalia Gebrial explains, Uber’s and Lyft’s deactivation systems draw on long-held, racially biased tropes of guilt and innocence to configure drivers—who are racialized and gendered as Black and Brown men—as being a “threat” or “risky,” and passengers—who are racialized as white and more likely female—as being “threatened” or “at risk.” Thus, while Uber and Lyft drivers must submit photo identification, pass driving, and criminal background checks, and satisfy other requirements, passengers can download the app and create an account without any such verifications. Similarly, while drivers can rate and report passengers for misconduct, this mostly does not result in deactivation.

Significantly, the asymmetric burden of compliance that app-based companies’ automated systems impose on drivers does not map onto the actual, relative health and safety risks to drivers and passengers using these platforms. Uber’s internal reports in 2019 and 2020 show that drivers are nearly as subject to assault from passengers as passengers are from drivers. Further, as sociologist Elizabeth Anne Watkins highlights, although many of Uber’s driver surveillance and management technologies were rolled out in the name of passenger safety, Uber has yet to publish any data on whether these interventions have had any impact on account fraud or passenger safety.

As described in an investigation by the non-profit news organization, *The Intercept*, recent artificial intelligence patents filed by Uber reinforce the company’s pattern of experimenting with algorithmic prediction and driver surveillance systems in the name of passenger safety. These

---

104 Ibid.
105 Driving Danger, supra, n. 45, p. 13.
106 D. Gebrial, supra, n. 3, p. 16.
107 Id., p. 16-17.
109 D. Gebrial, supra, n. 3, p. 17.
new systems also raise concerns that they could result in unjust or biased deactivations of drivers, including immigrants and drivers of color. One patent for scoring driver safety risk suggests a passenger’s reporting they could not understand the driver’s “heavy accent” can be an indicator of “low-quality” service.\textsuperscript{114} Another patent aims to predict safety incidents using criteria that include, among others, passenger ratings and a driver’s social network peers.\textsuperscript{115} But passenger reviews can be racist. And to the extent immigrant drivers and drivers are more likely to be socially connected to drivers living in lower-income neighborhoods, those neighborhoods tend to have a higher degree of traffic crashes than affluent neighborhoods, research indicates, not because of driver safety, but because of the greater prevalence of hazards in the built environment and of older vehicles without safety features.\textsuperscript{116}

Yet another Uber patent develops an individual “driver safety score,” which, if unsatisfactory, can be a basis for “intervention.”\textsuperscript{117} According to the patent, driving at night is a factor that could negatively impact a score, in comparison to driving during the day.\textsuperscript{118} But if drivers who drive at night are more likely to be drivers of color and immigrants because they tend to hold down multiple jobs or drive longer hours, these groups could theoretically be penalized with lower scores and be vulnerable to intervention.\textsuperscript{119}

As Gebrial highlights, the manufactured construction of app-based drivers as public safety threats is deployed to justify the logic that drivers’ behavior must be minutely quantified and subject to constant scrutiny.\textsuperscript{120} This surveillance apparatus provides the pre-conditions for Uber’s, Lyft’s, and other app-based companies’ swift and heavy-handed driver deactivations,\textsuperscript{121} which, in turn, create a more disposable, exploitable, heavily disciplined workforce of vulnerable Black and Brown drivers.\textsuperscript{122} Ironically, safety rhetoric becomes a way to make app-based drivers’ already risky jobs even more dangerous by subjecting them to ever more precarious working conditions.

**Federal Agencies Can Take Action Now**

While app-based companies’ automated worker surveillance and management systems may be relatively new, the social harms workers experience as a result of these practices—low and unfair pay, lack of benefits, biased and arbitrary discipline and firings, health and safety threats, and insecurity are not. Federal agencies can now take action to address these social harms through regulations, enforcement, contracting, and grantmaking.

**Policy, Regulation and Enforcement**

\textsuperscript{118} Ibid.
\textsuperscript{119} Ibid.
\textsuperscript{120} D. Gebrial, supra, n. 3, p. 18. Gebrial also notes the “parallels between the use of data-extractive algorithms to police racialised urban populations, and the algorithmic management of racialised urban workers.” Ibid.
\textsuperscript{121} Id., p. 17.
\textsuperscript{122} Id., p. 2.
Given the extreme lack of transparency in app-based corporations’ algorithmic decision-making and surveillance systems to workers and the general public, the federal government and other regulators are uniquely positioned to investigate abuses wrought by these corporations and enforce violations when found.

- **Issue Final Rulemaking on Classifying Employees, Independent Contractors:** The Department of Labor (DOL) should move forward expeditiously with final rulemaking on its October 13, 2022, Notice of Proposed Rulemaking (NPRM) on the classification of employees and independent contractors, including identifying automated worker surveillance in its discussion of control reserved or exerted through supervision.\(^\text{123}\)

- **Prevent and Address Antitrust Violations:** The Federal Trade Commission (FTC) should continue to prioritize preventing and remedying antitrust violations in the app-based economy, consistent with its September 15, 2022, *Policy Statement on Enforcement Related to Gig Work*.\(^\text{124}\) This includes but is not limited to investigating and enforcing unfair or deceptive practices involving automated or algorithmic decision-making.\(^\text{125}\)

- **Prevent and Address Consumer Violations:** The Consumer Financial Protection Bureau (CFPB) should continue to prioritize preventing, investigating, and remedying consumer violations in the app-based economy, including, but not limited to, certain actions by surveillance companies involving the tracking and sale of worker data may be violating the Fair Credit Reporting Act and other consumer financial protection laws.\(^\text{126}\)

- **Address Exemption for Worker Organizing Activities from Antitrust:** Consistent with the September 28, 2021, letter to Congress from FTC Commissioner Lina Khan and Commissioner Bedoya’s April 28, 2023, address, the FTC should work with the Department of Justice’s Antitrust Division to guide courts regarding the exemption of “worker organizing activities from antitrust.”\(^\text{127}\)

- **Convene an Interagency Task Force on App-Based Workers:** A Task Force should be created to identify federal agency policies, practices, and programs that could be used to promote app-based worker voice and job quality as well as to address harms to app-based workers—and particularly, workers of color—experience from automated management and surveillance systems. Some federal government agencies have taken some initial steps to prioritize these challenges, but these challenges are a matter of national interest, requiring a coordinated response.


\(^{125}\) Id., p. 10.


● **Launch a Gig Worker Outreach Initiative:** Consistent with their recent announcements to expand enforcement of app-based workers’ legal protections nationally, the DOL, the National Labor Relations Board (NLRB), the FTC, and the CFPB should: (1) expand national and regional outreach to app-based workers, and (2) post updated, visible, and accessible materials on agency websites, worker.gov, and social media platforms on app-based workers’ rights and on how to report potential workplace issues to the government.

**Contracting and Grantmaking**

● **Assist App-Based Platform Cooperatives:** Relevant agencies should invest in revolving loan funds or grant programs that make low- or no-cost financing available to worker-owned, app-based cooperatives and the technical assistance organizations supporting them.

● **Assist Workers Centers and App-Based Worker-Led Organizations:** Relevant agencies should invest in grant programs and app-based worker-led organizations to support workers' centers. These organizations relieve stressors on app-based workers by supporting connections to the social safety net, improving financial literacy, lessening social isolation, and educating and providing app-based workers with information on their rights.

● **Explore Opportunities for Enhancing App-Based Workers’ Job Quality Through Federal Contracting:** Relevant agencies should identify contracting opportunities where they can incorporate job quality elements, disclosure or information requirements regarding the use of automated management or surveillance systems, and other mechanisms to enhance job opportunities for app-based workers. Relevant agencies should also evaluate establishing procurement policies to provide preferential treatment of platform app-based cooperatives over privately owned app-based platforms.

As the federal government continues assessing automated surveillance and management systems, we welcome any future opportunities for collaboration. This includes offering analyses, resources, or guidance in developing policies, programs, and best practices. Thank you for your review and consideration of this response.

Sincerely,

The Action Center on Race & the Economy

---


129 A worker-owned, app-based cooperative is a website or mobile app designed to provide a service or sell a product that is collectively owned and governed by the people who depend on and participate in it. Platform Cooperatives, Univ. of Wisconsin Center for Cooperatives, https://tinyurl.com/5f2sutun (last visited May 30, 2023).

PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0195
Comment on FR Doc # 2023 12995

Submitter Information

Name: (b)(6) PII
Address: [Blacked out]
Email: [Blacked out]

General Comment

I am filing a comment on behalf of myself, a worker with US labor agency charges & cases that involve critical public policy concerns about worker surveillance and electronic monitoring. Please see attached memo in response to this request for information.

Attachments

OSTP(b)(6) PII Comment 2023
Request for Information:

Automated Worker Surveillance and Management

Federal Register No. 2023-12995
Doc ID: OSTP_FRDOC_0001-0008

U.S. Office of Science and Technology Policy

Information

Associated Cases:

U.S. Department of Labor:
(b)(6) PII

U.S. National Labor Relations Board
NLRB v Apple (b)(6) PII

California Department of Labor:
(b)(6) PII

Associated Investigations:

U.S. National Labor Relations Board
Charge No. (b)(6) PII (Division of Advice & Region 31)

U.S. Federal Trade Commission
Report No. (b)(6) PII

U.S. Securities & Exchange Commission
Tip No. (b)(6) PII (SF Regional Office)

German Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Complaint No. (b)(6) PII (Bavaria Office)
# Table of Contents

**Introduction**

- Apple’s Culture of “Loyalty” & Intimidation .......................................................... 6

**Electronic Monitoring & Data Collection**

- “Face ID” & Apple’s Face “Gobbler” Application ....................................................... 12
- Ear Studies ..................................................................................................................... 27
- Other User Studies ........................................................................................................ 30
- Radar & Sysdiagnose ................................................................................................... 32

**Secrecy** ....................................................................................................................... 33

- Secrecy Policies .......................................................................................................... 33
- Search and Privacy Policies ........................................................................................ 35

**Public Policy** ............................................................................................................... 40

**Conclusion** .................................................................................................................. 46

*Originally Submitted as “Complaint For Invasion Of Privacy” in April 2022; Revised for OSTP in June 2023*
June 29, 2023

To Whom it May Concern,

The United States' legal protections for human rights at work lags far behind countries in the European Union, especially France and Germany. Similarly, national legal protections for digital privacy are basically non-existent in the United States and are decades behind other nations.

Over the last few years, we have witnessed increasing surveillance, electronic monitoring, and digital exploitation of workers in the United States. We have also seen an increasing number of requests from politicians, agencies, unions, and civil society asking the US government for legal protections for workers.

Despite numerous and persistent requests from Senators,1 NGOs,2 unions, and from workers themselves3 – there is no progress to be seen. Despite a number of agency memos4 and social media posts, we have yet to see any new legal protections or even any meaningful enforcement of violations of existing laws.

While you will likely receive comments and information from groups with more expertise on the history, policy, and legal landscape of this topic – what I can offer you is a first-hand case study in failure.

My story as a worker in the United States, for one of the biggest companies in this country, highlights the lack of legal protections for workers, the lack of express privacy protections for citizens, and the lack of any actual enforcement mechanism even for egregious violations of the narrow privacy/labor laws we do have on the books today. My story also highlights how my employer understood this current landscape and thus acted with an aggressive...

---

3 TechCrunch, Ex-Apple employee takes Face ID privacy complaint to Europe, April 11 2022, https://techcrunch.com/2022/04/11/gobbler-complaint-europe/
disregard for the law, ethics, or social norms. So far, they were right & they have faced no consequences.

In March 2022, I received a written statement from my employer’s lawyers admitting they fired me (with multiple federal investigations already open due to my charges against them for whistleblower retaliation, environmental and labor violations, and fraud); but claiming I was not fired in retaliation for that, but instead fired for supposedly ‘legal’ retaliation for my protests of their unlawful surveillance of employees, their intimidation and censorship of employees, and their coercive harvesting of sensitive worker information in order to build their products (in ways that they admitted in writing that would be illegal in France of Germany). In response, in addition to complaining further to US agencies, I also filed a complaint to other countries where my ex-employer has large offices.

Despite overwhelming evidence and even a written confession admitting what my employer has done, my charges have sat with federal agencies for nearly two years now gathering dust. Despite my being a US citizen and all of this occurring within the United States, as far as I can tell, there has been more progress investigating my claims in Germany then there has been in the United States.

Introduction

I worked for Apple as a Senior Engineering Program Manager During my tenure with Apple, I participated in engineering project management of numerous high-profile products such as the iPhone, iPad, iPod, Apple Watch, MacBook Pro, MacBook Air, Mac Pro, iOS, macOS, watchOS -- and high-profile projects/programs such as the launch of the Apple Music subscription service, Apple’s transition of computers from Intel to Apple silicon, and the development of a company-
wide Artificial Intelligence ethics policy. I was told by my Apple managers that I was both “key talent” (irreplaceable) and a “high performer.”

In August 2021, I expressed public concerns about Apple’s overly restrictive and invasive employee policies, and Apple pressuring its employees to participate in invasive data collection procedures, including scans of ears/ear canals (which I believed captured employee data that could be used for biometric identification and mass surveillance). I also raised concerns about an iOS application (the Face “Gobbler”) on employees’ iPhones that automatically took photos/videos whenever it “thought it saw a face.”

I raised concerns about Apple’s unlawfully invasive “Search and Privacy Policy” for employees, Apple’s limitless access to employees’ personal iCloud/Apple-server-based data, and Apple’s culture of intimidation and secrecy including a private police force with access to all of the above data.

Apple terminated me on September 9 2021 for reasons unknown to me at that time but assumed by myself and the press to be retaliation for my protected activities (I had filed labor and retaliation charges with the U.S. government only weeks earlier; and the US EPA demanded an inspection of my Superfund office due to my disclosures, conducted the inspection and found CERCLA non-compliance issues also only weeks prior).

Apple contacted me via external lawyers a week after I was fired to complain about several Twitter posts I made. Suggesting these posts were the reason for my termination was so farfetched & pretextual that a detailed article was written about it, titled “Apple Wanted Her Fired. It Settled on an Absurd Excuse.”

Last year, Apple offered their explanation for my termination to the U.S Department of Labor (in response to my allegations of federal whistleblower retaliation in violation of SOX,
INFORMATION FOR OSTP ON AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT IN THE UNITED STATES

CERCLA, and OSHA statutes).\textsuperscript{13} Apple doubled down on the “absurd excuse” & cited my opposition to their harvesting of employee biometrics and their secret, invasive photography of employees as a legitimate justification for my termination.\textsuperscript{14} I am now even more concerned knowing Apple felt comfortable telling the U.S. government that they believe their unlawful invasion of employee privacy is “legitimate” and any employees who protest privacy invasions deserve to be terminated, as I was. Any argument Apple had that employees consented to these practices was thrown out the window when they formally claimed I was terminated without warning for protesting those practices.

APPLE’S CULTURE OF “LOYALTY” & INTIMIDATION

I will describe some of these practices which Apple claimed were so secret, they’d terminate an employee for protesting and exposing them. However, first, it is important to establish that at Apple, there is a long-standing tradition that workers keep their mouths shut, do what they are told, and be ‘loyal’ to the company above all else.

GDPR recognizes that employment relationships are inherently coercive and thus employees cannot provide meaningful consent to invasive surveillance and data collection practices. In the US, we sometimes still default to a neoliberal view that a ‘request’ or ‘preference’ from an employer is somehow optional and thus employees have agency to decline. This is not accurate and Apple provides an incredible example of how many US companies operate but may be too afraid to explain aloud. Apple says the quiet parts aloud because they have terrorized their employees to the extent Apple was sure their employees would not report the misconduct.

In stark contrast to international labor standards, Apple’s “Worldwide Loyalty Team” “does KGB-style lockdowns [of employees] and Gestapo interrogations that end in suicides.”\textsuperscript{15} The team is an “internal secret police team known for its network of informers, and ruthless,

\textsuperscript{13} Patrick McGee, "Apple faces probe over whether it retaliated against whistleblower," Financial Times, Dec 13 2021, https://www.ft.com/content/973ae8d-21d9-4e84-8912-ead071c7935d

\textsuperscript{14} [b|(6) PII]

systematic pursuit of leakers.” Among some employees, they are known as the “Apple Gestapo,” a group of moles always spying in headquarters and stores, reporting directly to the CEO.” Apple holds out its security policies out as “voluntary” meanwhile: “management recommends that you relinquish your phones. If you don’t do it they will fire you, or they will investigate why you didn’t want to give them your cellphone.”

Apple’s Global Security team has a sketchy history, including Apple employees accused in 2011 of impersonating policemen and searching a man’s San Francisco home for a lost prototype, and threatening to have the man deported if he did not cooperate. Apple was also accused in 2010 of violating California’s shield law with an illegal search warrant, when they searched the home of a journalist, again looking for a prototype. Gawker described Apple’s secret police as “sleazy.”

Apple employees’ experience with this Gestapo have been described by the press as “knowing how it feels to be watched, to always be considered guilty of crimes against another kind of state. Knowing how it felt to have no privacy whatsoever when he was working right here, in a little Californian town called Cupertino, in a legendary place located in One Infinite Loop.” Indeed, a few years later an ex-Apple executive described the culture at Apple as “everything is on a need-to-know basis” and that Apple has “cells, like a terrorist organization.”

Further, while some Apple employees may report an earnestly positive experience, the company is large and has decades of history of very negative experiences for many others. Apple has gone to great lengths to conceal and cause society to forget its bad behavior. Apple has a

---

Apple workers around the globe have been involved in organizing since at least the 1990s. Apple worker organizations have been made up of retail, corporate, contract, and other workers. Unionization efforts started in the United States back in 1991 with Apple’s janitors successfully unionizing with SEIU through protests, boycotts, press coverage, and even a hunger strike. In 2013, retail workers started organizing a “Apple Retail Workers Union” and calling for a formal labor union. Apple security guards started organizing and looking to form a union in 2014.

---

29 NBC News, “Chinese factory asks for 'no suicide' vow,” 2010, nbcdn.com/id/wbna37354853
with SEIU. At that time, a USWW union executive complained, “Apple frequently intimidates workers and retaliates against those who get involved with the union around the country.”

In 2015, Apple shuttle and bus drivers successfully unionized with the Teamsters. Starting in 2022, numerous Apple Retail Stores in the US have attempted to unionize. Union-busting tactics were already reported early on. Apple retail store employees in Atlanta Georgia withdrew an election citing ‘illegal union-busting tactics’ by Apple. “Apple has conducted a systematic, sophisticated campaign to intimidate them and interfere with their right to form a union,” the CWA representative said. NLRB General Counsel found merit Apple was unlawfully forcing workers to attend captive audience meetings. In September 2022, an Oklahoma City Apple retail store petitioned for an election, represented by CWA, and voted to unionize in October of 2022. They also filed charges with the NLRB against Apple for “illegally surveilling, threatening and questioning workers at the Oklahoma City store.”

In October 2022, the NLRB issued a complaint against Apple over accusations that Apple interrogated its retail workers about their union support and prevented pro-labor fliers in a store break room. The union accused Apple of interrogating staff at a World Trade Center store and

---

38 Some U.S. Apple Store employees are working to unionize, part of a growing worker backlash, Washington Post, Feb 18 2022, https://www.washingtonpost.com/technology/2022/02/18/apple-retail-stores-union-labor/
39 Some U.S. Apple Store employees are working to unionize, part of a growing worker backlash, Washington Post, Feb 18 2022, https://www.washingtonpost.com/technology/2022/02/18/apple-retail-stores-union-labor/
discriminating against union supporters in enforcing a no-soliciting policy. In June 2023, an NLRB judge ruled against Apple, finding Apple violated federal labor law. In December 2022, Apple retail workers organizing with CWA in Columbus Ohio filed a complaint to the NLRB alleging Apple was “soliciting employees to join an employer-created / employer-dominated labor organization as a means of stifling union activities” (aka an unlawful company union) in addition to holding captive audience meetings and making threats. In December 2022, NLRB found merit that Apple violated the NLRA in Atlantic Georgia. In January 2023, NLRB found merit in five unfair labor practice charges filed by corporate employees.

In China, Apple directly employs 12,000 workers across its retail and corporate divisions and claims agency over 4.8 million workers in the country; likely most are contracted through Apple’s suppliers and manufacturing plants, including at least 1.2 million working at Foxconn’s iPhone assembly factories. Foxconn is the largest unionized company in the world. Foxconn made global headlines with a wave of worker suicides at the company’s Chinese plants in 2009 and 2010, and after its treatment of its huge workforce has attracted intense scrutiny. Foxconn and Apple’s response to the suicides was to have large nets installed outside many of the buildings to catch falling bodies (“suicide nets”), and workers were made to sign pledges stating they would not attempt to kill themselves. Foxconn has become a focus for criticism of practices widespread in Chinese factories including illegal overtime, low pay, and the use of underage workers. Even last year, Foxconn’s Apple factories were in the news again – now with allegations of indentured servitude and

---

trafficking, and when workers protested the abuse, they were met with beatings by state police.\(^5^4\)

On December 18, 2014, retail workers in Apple’s Japan stores announced a union affiliated with Tozen. Three of Japan’s ten Apple stores are now unionized with Tozen.\(^5^5\) There have also been unions and worker protests in India. In December 2020, thousands of contract workers at a Bangalore factory owned by Apple supplier Wistron Corp protested over alleged non-payment of wages.\(^5^6\)

Other violations highlighted found upon further investigation included underpayment of wages to contract workers and housekeeping staff, and making female staff work overtime without legal authorization.\(^5^7\) In December 23 2021, 159 workers protested for poor working conditions and a mass poisoning incident.\(^5^8\) Twenty-two activists, including leaders of the Centre of Indian Trade Unions (CITU), were put behind bars for extending support to the workers and visiting them.\(^5^9\)

In September 2022, Australian workers brought Apple to the Fair Work Commission over employee demands for better pay and a guaranteed weekend.\(^6^0\) The workers secured a protected action order with the nation’s Fair Work Commission, which would allow them to protest without risking their jobs or getting sued.\(^6^1\) The national secretary of the SDA Union, accused Apple of acting like “a cheap bully in a cheap suit” and said it never should have taken intervention from the Fair Work Commission for Apple to come to the table. “This giant multinational should have more regard for the welfare of its Australian workforce than to try to dictate a pre-determined outcome it wants to impose rather than engaging in genuine bargaining. This is Australia not the United States,” he said.\(^6^2\) In October 2022, with three Australian unions negotiating with Apple for better pay,


\(^5^7\) Apple puts supplier Wistron on notice after Indian factory violence, Reuters, December 19 2020, https://www.reuters.com/article/apple-india-idCAKBN28T0DW


\(^6^1\) Australian Workers Are the Latest International Apple Staff to Unions, VICE, September 8 2022, https://www.vice.com/en/article/qjk3eb/australian-workers-union-apple-strike

benefits, and working conditions – 150 workers engaged in a strike.63

Apple is a huge multinational corporation based in the United States with a long history of labor and human rights violations in their domestic and international supply chain and operations. If Apple is not held accountable in the country the corporation is headquartered in, what hope do other countries have in enforcing international labor standards against Apple abroad? The United States must set expectations for Apple here & abroad – that whether it is California labor and privacy laws, United States labor statutes, foreign national labor laws, or international standards such as from the International Labor Organization – whether it is employees, contractors, or vendors – Apple should be expected to made a good faith effort to follow the law, and governments should be able to investigate allegations of misconduct with independence and integrity. But that is not occurring; enter, my case study.

**Electronic Monitoring & Data Collection**

**“Face ID” & Apple’s Face “Gobbler” Application**

Apple announced its “Face ID” iPhone authentication feature on September 12, 2017.64 Face ID captures, collects, and possesses Face ID users’ facial geometry by “*projecting and analyzing tens of thousands of invisible dots to create a depth map of [the user’s] face and also captures an infrared image of [the user’s] face.*”65 Face ID data is “*refined and updated as [users] use Face ID.*”66 Apple says their average users unlock their phones 80 times a day, but other reports state people look at their phones upwards of 130 times a day.67 Apple says Face ID is “*attention aware*” and only unlocks an iPhone when the user’s eyes are open and looking at the screen.68

---

64 Apple announced Face ID during the unveiling of the iPhone X on September 12, 2017, [https://www.theverge.com/2017/9/12/16288806/apple-iphone-x-price-release-date-features-announced](https://www.theverge.com/2017/9/12/16288806/apple-iphone-x-price-release-date-features-announced)
Privacy concerns arose quickly after launch, the security of biometrics gathered/stored by Face ID. App developer access to iPhone X face data spooks some privacy experts, https://www.reuters.com/article/us-apple-iphone-privacy-analysis/app-developer-access-to-iphone-x-face-data-spooks-some-privacy-experts-idUSKBN1D20DZ

Privacy concerns arose quickly after launch, the security of biometrics gathered/stored by Face ID. TechCrunch wrote, “Face ID raises a range of security and privacy concerns because it encourages smartphone consumers to use a facial biometric for authenticating their identity and specifically a sophisticated full three-dimensional model of their face.” Concerns were also raised the year before about Apple’s “faceprints” in its Photos applications. The Verge wrote, “There’s a real privacy issue at stake... Facial recognition can be put to some very creepy uses when faceprints are freely available.”

A researcher warned in 2017, “once the Face ID system is enabled, the iPhone X can become a potential technology for users to be spied on without noticing. Information about faces can contain a lot of personal information like age, gender, race but also emotions. Face ID can recognize these emotions and this information can for example be combined with on-screen content like advertisements and websites. Face ID technology might also ‘read’ the environment of the iPhone’s user. The technology might be aware of the user’s specific living conditions.”

In 2017, Senator Al Franken wrote to Apple (via Tim Cook), expressing concerns and requesting clarifications about the privacy of Apple’s Face ID feature. Apple responded saying, “Face ID uses facial matching neural networks that we developed using over a billion images, including IR and depth images collected in studies conducted with the participants’ informed consent.” Meanwhile, however, Apple was pressuring employees to upload their “faceprint data” to Apple internal servers, capturing secret photographs and videos of employees, and told employees that face-related logs were automatically uploaded from their iPhones daily. Further, with Apple’s internal Mobile Device Management (MDM) profiles and other security tools, it’s doubtful whether the data would even need to be “uploaded” or if Apple already had access if they wanted it.

---

69 App developer access to iPhone X face data spooks some privacy experts, https://www.reuters.com/article/us-apple-iphone-privacy-analysis/app-developer-access-to-iphone-x-face-data-spooks-some-privacy-experts-idUSKBN1D20DZ
72 Amber de Zeeuw, iPhone Face ID: Privacy issues we should worry about, 2017, https://mastersofmedia.hum.uva.nl/blog/2017/09/25/iphone-face-id-privacy-issues-we-should-worry-about/
In 2017, Craig Federighi said that because “the [Face ID training] data needed to include a high-fidelity depth map of facial data,” “Apple went out and got consent from subjects to provide scans that were quite exhaustive. Those scans were taken from many angles and contain a lot of detail that was then used to train the Face ID system.”  

On Jan 9 2019, the Apple manager running Gobbler, posted an article to LinkedIn called “Data Collection” where he wrote, “During the lead up to Face ID being launched, my team went out and collected a large set of potential aggressors to see if we were missing anything in our larger data collections, things would be normal to a regular user.” Later that year, he posted again about the work Apple did on Face ID, saying that “tons of data was being collected at the time to cover all the bases.”

In 2017, Craig Federighi said Apple “went to great lengths to gather its own data on facial shapes and angles.” Federighi said, Apple “retains a high-fidelity depth map of that [training] data” and “as Apple trains these models and iterate on these algorithms,” Apple “wants raw sensor data to use and develop and optimize them.” Federighi, said “When it comes to customers, Apple gathers absolutely nothing itself via Face ID and that Apple does not gather customer data when you enroll in Face ID, it stays on your device, we do not send it to the cloud for training data.” Federighi did not distinguish a customer in range of the hot & hungry camera of an Apple employee’s iPhone with Gobbler installed.

Apple never responded directly to one of the Senator’s questions, either to the U.S. Senate or to the press. The Senator asked, “Apple has stated that it used more than one billion images in developing the Face ID algorithm. Where did these one billion face images come from?” Apple would not answer. What Federighi omitted is that those images came from employees just like me, whether I wanted to share them or not.

---

76 LinkedIn, https://www.linkedin.com/pulse/design-experiment-data-collection-robert-mckean-aloë/
77 LinkedIn, https://www.linkedin.com/pulse/ml-examing-test-set-robert-mckean-aloë/
The Gobbler User Study

I worked in Apple Research & Development. We were frequently pressured to “live on” one device for both work and personal use. Apple wanted to use our uncompensated labor to test new hardware and software using customer scenarios 24/7, at the expense of our privacy and work/life balance. This extended to my “live on” and testing of these devices, with my personal data and usage, being cited in my annual review. I even received emails noting what device I was ‘living on’ and nagging me to move to a future software build or prototype hardware model. We were also pressured to participate in very personal “user studies” using company devices.

On August 3 2017, an Apple engineering manager emailed an unknown list of Apple employees, including myself, about a “Gobbler” user study.82 The manager wrote the study used an iOS application called “Gobbler,” and told employees “as you continue to use your device, use the Gobbler application to periodically upload data that has been logged.”83 The manager then wrote, “**In terms of data collection, we want more.** The algorithm uses deep learning and the more data the better.” He wrote that the Gobbler algorithms are “**hungry for data**” and that “for uploading data: all data that has your face in it is **good data.**”84 I did not respond to or act on the email; it was a weird email and by the way it was described, I wanted nothing to do with that tool/study, even if it meant I was being ‘disloyal.’

On Aug 7 2021, I received a different email from a group account saying “**Come join us! We look forward to seeing**

---

82 Email from R.M. in Apple Video Engineering, to “recipients not specified,” Date: August 3 2017 7:45am PST, Subject: Participating in [codename]Loop...

83 Email from R.M. in Apple Video Engineering, to “recipients not specified,” Date: August 3 2017 7:45am PST, Subject: Participating in [codename]Loop...

84 Email from R.M. in Apple Video Engineering, to “recipients not specified,” Date: August 3 2017 7:45am PST, Subject: Participating in [codename] Loop...
you there!” 85 The email appeared to be a mandatory social event, though I was confused why the email said not to attend if I was "taking photosensitizing medications or have any known photosensitizing medical conditions." Regardless, I promptly accepted, assuming it was expected of me. (The message said nothing about Face ID.) I received another response later that day saying, “Hello there! Thank you very much for responding to our invite! ..... You will receive an iCal invite to the event shortly... Please arrive at [Apple's Mathilda 3B office building] Patio at your scheduled time. Do not hesitate to reach out if you have any questions or concerns regarding the study. See you soon!” 86

It still sounded like some sort of mandatory social event, however the email also stated “Prior to your participation, we kindly request that you do the following: Review the ICF [Informed Consent Form] and email sign the ICF by registering your email and completing the short pre-study survey that will be sent.” During my time at Apple, I was forced to sign hundreds of contracts to get access to everything from offices, conference rooms, documentation, and the basic to do my job, so I “signed” the ICF as requested. As far as I can tell, I never received a confirmation I signed it, nor did I get a copy of the ICF, and when I tried to access the ICF 87 again in 2021 the link went to website with an error message saying “connection insecure.”

I showed up to the “Social Event” as requested. The “patio” was actually a parking lot. The temperature that day was very hot. As I approached the destination, if my memory serves me right, I saw a ~40ft diameter circular compound, with ~10ft high fence around it. There was a chain link fence, with black plastic lining it and then another chain link fence and more black plastic. On top, there were security cameras pointed inside and outside. There were one, maybe two, armed security guards standing outside the compound. One of the guards checked me in and told me to sit at a picnic table until called. I remember being hot, dehydrated, and scared. I wanted to leave, but didn’t want to ask to leave, because then the armed guard might get upset or suspicious, so I waited. They finally let in 4 or 5 employees. They opened the first door of the gate, we went in, then they close the outer gate and open the inner gate – so no one on the outside could see in. I believe the gate was locked behind us.

85 Email from SSP User Study Group to “recipients not specified,” Date: August 7 2017 7:45am PST, Subject: Social Hour Study: You’re Invited!
86 Email from SSP User Study Group to “recipients not specified,” Date: August 7 2017 6:55pm PST, Subject: Social Hour Study: Registration
87 “Attach” link
Upon entering, there was music playing in the background & we were told to sit in the circle. The armed guard left and there were two Global Security guys remaining. One was at the make-shift bar & the other guy sat with the employees in a circle. I wanted to leave but I was locked in a compound with 10ft high gates, security cameras, and an armed guard, so I thought “I’m too young to die” and stayed put.

The guy in the circle explained what we’re doing, we’re going to enroll in Face ID and we're going to test it on iPhones with this Gobbler application and we must complete a set list of testing objectives before we are allowed to leave. The ICF had to be complete before we could set up the accounts, and he helped us set up the Gobbler accounts on the test phones. Then we had to try to enroll in Face ID and then complete our task list. It was like 12 tasks (put sunglasses on & take 10-20x pics, make a “silly” faces & take 10-20x pics, etc). He explained this testing set-up was specifically because they were having trouble with direct sunlight conditions, so even though they wanted to keep all testing in secure lockdowns, they set up this compound in the 100-degree sun so we could do real world testing for them.

I remember being miserable and desperately wanting to leave, so I did the testing as quickly as I could so I could go. When each of employee was done, I remember the guard unlocked the inner gate, then had the employee step in, closed the inner door, and opened the outer door and let them out. After that, the Gobbler application was always pre-installed and logged in on my iPhone, even if I changed phones. I kept attempting to log out and turn it off, but it would keep reopening and logging back in and collecting more videos/photos.

Apple would later rename the application from Gobbler to “Glimmer” after criticism about the facial “Gobbler” name. On Apple’s internal “Living On” help page, it explains that when you “live on” Apple devices, “You are encouraged to make full use of your living on devices as you regularly would, and try to log as many bugs as possible. This will help us provide a better and bug free product to our users.”
The page also has a section on Gobbler/Glimmer, explaining “Glimmer is an app that's included in internal development installs of Face ID equipped devices.”

The page suggests uploading data from the app “captured in employee’s homes.” Apple’s internal “Face ID FAQ” page said “Users are encouraged to use Face ID in all places Touch ID is replaced on iPhone X….please use in a variety of conditions: From the bright outdoors to the darkest rooms. In workday, evening and weekend attire. With and without makeup.” It said the Gobbler data “can be previewed and included in radars and/or donated otherwise via the Gobbler to help make the feature better (there are many other things besides training the neural nets, that the data can be used for to improve the product).” The page did not elaborate further.

In the documentation pages, several restrictions were noted. One said, “Data gathering may be restricted in some countries. You will be notified if that is the case.” Another said, “Data privacy laws only allow us to gather and upload data from the US, Canada or Israel. Please do not upload any data gathered outside of these countries.” Another said, “To participate, please take the time to download the Informed Consent Form... and review it.” The Apple manager said the study was being conducted in “the USA, Brazil, Tel Aviv,” and the EU “but not France or Germany.” A page said, “some data should not be submitted from certain regions,” while another page said, “For now, Glimmer is only available for Apple employees working in the United States.”

I also saw in notes that the app was forbidden to be used in Japan and China, but then at some point, Apple decided to gather some logs there anyways. On October 16, 2019 an engineer filed a Radar titled, “Add Geo Location into Glimmer,” saying

“We're going to change how we deal with blacklisted countries. We're going to allow auto-A files to upload…. The aim is to better understand Japan and China because we have a number of people over there know...We’re adding another

---

88 Apple, Living On, Dev Pubs, Confluence page
89 Apple, Using Glimmer, Confluence page
90 Apple, Using Glimmer, Confluence page
91 Apple, Face ID FAQ, Confluence page
92 Apple, Face ID FAQ, Confluence page
93 Standard Operating Procedure (SOP) for Glimmer usage
94 Apple, Face ID FAQ, Confluence page
95 Email from R.M. in Apple Video Engineering, to “recipients not specified,” Date: August 3 2017 7:45am PST, Subject: Participating in [codename] Loop...
96 Apple, Living On, Dev Pubs, Confluence page
97 Apple, Using Glimmer, Confluence page
field… specifying geo location is needed for distinguishing the location. Once the ICF is updated, the geo location for all previous black-list countries as China and Japan can also collect autoAF data.”

The engineer noted the changes were made as of Glimmer v3.25.0 on Dec 3, 2019.

It was extraordinarily unclear what data was being automatically uploaded, how and when. I saw another employee complaining in 2019, “why is Glimmer always running?” The engineer responded, “Glimmer is launched every day at 2 am to collect non-PI logs from FaceD, zip them, and upload them to a server for machine learning algorithms and data analysis tools to be computed. This allows to monitor non-regression and algorithm updates impacts.”

Another employee asked in 2019, “Why is Glimmer launching automatically?” He wrote, “I noticed on my device there’s some kind of launch job started by root to launch Glimmer as suspended all the time. Why is this happening? What is it for?” The engineer responded, “Glimmer is launched to upload some non-PI (logs) data automatically.”

My open questions included whether my personal data was being backed up on employee iCloud backups, synced via iCloud, and/or accessed/copied by Apple’s corporate MDM profiles – or other Global Security surveillance of employee phones. It also disturbed me that the app was taking photos/videos without any notification (sound, signal, etc), which made me think that Apple, if it wanted to, could activate my device cameras and watch me without me knowing at any time as well. I talked to other employees, including managers, with similar concerns.

---

98 Radar filed on October 16, 2019 at at 4:35 PM, Title: Add Geo Location into Glimmer
99 Radar filed on October 16, 2019 at at 4:35 PM, Title: Add Geo Location into Glimmer
100 Radar filed on December 13, 2019 at 6:08 PM, Title: Why is Glimmer always running?
101 Radar filed on December 13, 2019 at 6:08 PM, Title: Why is Glimmer always running?
102 Radar filed on September 25, 2019 at 1:53 PM, Title: Why is Glimmer launching automatically?
The article discussed the Gobbler app and that “images are recorded every time employees open their phones” and “every time an employee picked up their phone, the device recorded a short video — hopefully of their face.” The article quoted the internal email saying “all data that has your face in it is good data,” “If they did this to a customer, people would lose their goddamn minds,” The article noted that two employees confirmed that participation in studies like Gobbler was not just “encouraged” but “even expected.” The article also noted employees had no idea “what was happening with the hundreds of images” taken by their phones.

INFORMATION FOR OSTP ON AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT IN THE UNITED STATES

The Twitter Posts

Twitter Post: August 30 2021

^ The Twitter Posts ^

Twitter Post: August 30 2021

(b)(6) PII

(b)(6) PII
I still love #Apple products & brand. I devoted nearly 7 years & much blood/sweat/tears ensuring Apple's products are exceptional. However, Apple the corporation needs a reckoning. Apple's policy of "secrecy" should not shield it from public scrutiny about human rights & dignity.

Working at Apple in "normal" times, I walked in circles around their glass-walled panopticon, only able to badge into select lock downs (a constant reminder that Apple has absolute control over my resources and access), and was immersed in a culture where it is implicitly forbidden to critique Apple policies or even speak openly to your coworkers with concerns about your employment & work conditions, lest you upset the cronyism, ex-CIA/ex-FBI security teams, and other "powers that be." I realize now that during those times, I didn’t question a lot of things that I should have. Not just the abuse I suffered, but also the constant invasion of privacy — and perhaps those two things are linked.

There seems to be limitless ways Apple can access employee data and monitor us. I recently shared how violating it felt for Apple to demand to copy & permanently store my nudes for completely unrelated litigation. After the public outcry, I questioned other policies & actions Apple had taken. The internal "Glimmer" app had always troubled me, but I never voiced that concern, because inside we don’t question the way things are or what we’re asked to do. But now, in the light of day, considering everything Apple’s already done to me, this app, the photos & data it gathers, and how little we know about what it does with all of that — is deeply troubling and I felt compelled to make it public. Apple’s policy of “secrecy” should not shield it from public scrutiny about human rights & dignity.
Responses to my disclosures included, but were not limited to:

- “This is creepy. I don't have words to express what is running through my head.”

- “Straight up abusive and creepy behavior how can deployed iOS devices even run stuff like this?”

- “Whatttt” & “What the hell….” & “Excuse me WHAT”

- “Ah, but does the employee handbook say workers are human?”

- “I've heard a manager say we don't have civil rights as employees”

- “if anyone talks about apple privacy. show them this”

- “No, just no.”

- This entire article is.. wow.

- Because privacy is a fundamental human right that you need to give up to work for the company that cares so much about privacy.

- [insert su referencia a 1984 aquí]

- This is terrible and so bothersome on many levels.

- Quel enfer...

---

The “Gobbler” applications attempted to access my fully personal iPhone, even after I was fired.
In 2010, the Electronic Frontiers Foundation wrote an article about Apple seeking a patent to do just the kind of thing the “Gobbler” application does today. EFF called the technology “spyware,” “traitorware,” and “especially creepy.”\textsuperscript{124} EFF warned the patent provided “a roadmap for how Apple can — and presumably will — spy on its customers and control the way its customers use Apple products.”\textsuperscript{125} The technology would allow Apple to record the voice of the device’s user, take a photo of the device’s user’s current location or even detect and record the heartbeat of the device’s user.\textsuperscript{126}

EFF called the technology “dangerous” and warned, “this patented device enables Apple to secretly collect, store and potentially use sensitive biometric information about the user.” The patented technology can: “take a picture of the user’s face without a flash, any noise, or any indication that a picture is being taken to prevent the current user from knowing he is being photographed" and “can take a photograph of the surrounding location to determine where it is being used.”\textsuperscript{127} EFF warned, “Apple will know who you are, where you are, and what you are doing and saying and even how fast your heart is beating.”\textsuperscript{128}

“Apple does not explain what it will do with all of this collected information on its users, how long it will maintain this information, how it will use this information, or if it will share this information with other third parties.”\textsuperscript{129} EFF urged, “This patent is downright creepy and invasive…. Spyware, and its new cousin traitorware, will hurt customers and companies alike — Apple should shelve this idea before it backfires on both it and its customers.”\textsuperscript{130}

In 2010, \textit{Inc} also wrote about Apple’s “spyware” patent,\textsuperscript{131} calling it “creepy” and “Orwellian.” The reporter said concerns may vary based on how much users trusted Apple and how intimate their “relationship is with a faceless mega-corporation.” The writer queried readers, “Are you comfortable enough with Apple that it’s okay for them to have the power to turn on your iPhone camera, snap a picture of whatever is in plain site of the lense and then upload it to Apple for analysis?” And if you respond that yes you think that’s fine, then what if “... it’s all a big misunderstanding and the camera takes a picture for the Apple mothership while you are in...”

\textsuperscript{131} Patent: Systems and methods for identifying unauthorized users of an electronic device (10657238)
“Apple filed another patent in 2011 for iPhone remote surveillance capabilities, such as transmission of the images and sounds that the device secretly captures.”

Courts have acknowledged the intrusive effect of hidden cameras and video recorders in settings that otherwise seem private. It has been said that the “unblinking lens” can be more penetrating than the naked eye with respect to “duration, proximity, focus, and vantage point.”

On March 4 2022 Apple (via Orrick lawyers) wrote to the U.S. federal government that:

---

133 9to5 Staff, Patent indicates sophisticated remote surveillance for Find My iPhone, (Jun. 16th 2011), https://9to5mac.com/2011/06/16/patent-indicates-sophisticated-remote-surveillance-for-find-my-iphone/
135 (b)(6) PII
INFORMATION FOR OSTP ON AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT IN THE UNITED STATES

Apple’s Face “Gobbler”

- Page 26 of 47 -
969
EAR STUDIES

On Aug 10 2018, I was invited to a “HE User Study” for “anthropometry HH” sent by two Apple employees who previous asked for photos of my ears, and had discussed wanting to take scan my ears. I replied declining “indefinitely.” I assumed I’d be taken off the list for ear studies, but then in 2021, while I was on Indefinite Administrative Leave in August, I received three separate emails from Apple asking to scan my ears/ear canals, again. The email was titled, “HE 3D Ear Scan Invitation!”

The emails said, “You’re invited to a voluntary in-person study where we will capture high-resolution 3D scans of participants’ ears. The goal of this effort is to collect representative ear geometry data across age, gender, and ethnic groups. These 3D scans are extremely valuable to audio research efforts and better our understanding of ear geometry variance.” The email said I’d be asked to review an ICF prior to taking a recruitment survey and then another ICF for study participation. I did not respond to any of the emails nor did I sign any ICFs.

I was disturbed by Apple’s lack of respect for the privacy of its employees. I also wondered if Apple may have been emailing me these on purpose, since I already opted out, in order to harass me further. The emails didn’t say “Apple Confidential,” nor did they include anything that appeared actually secret or material. Regardless, I redacted them heavily when I publicly complained about the matter, since my point was to protest an employer pressuring its employees to gather such sensitive information (biometrics).
“I’m still over here in Apple’s time-out chair & they keep telling me to respect my abuser’s privacy & be silent. Meanwhile I got 3x of these in the last month since being on leave. NO, APPLE, STOP IT 😞
I can't tell if they're harassing me or just being super intrusive or both.”
Further, this wasn’t news. On September 5 2020, Apple VP of Marketing, Greg Joswiak (“Joz”) was interviewed by Wired about Apple AirPods.139 Joz said, “We did work with Stanford to 3D-scan hundreds of different ears and ear styles and shapes in order to make a design that would work as a one-size solution across a broad set of the population,” Joswiak says. “With AirPods Pro, we took that research further – studied more ears, more ear types. And that enabled us to develop a design that, along with the three different tip sizes, works across an overwhelming percentage of the worldwide population.”

On December 9 2021, two Apple Product Design executives were interviewed by Wallpaper about Apple’s product design team.140 The article said, “When AirPods’ development began a decade or so ago, human factors researcher Kristi Bauerly found herself researching the ‘crazily complex’ human ear. ‘We moulded and scanned ears, worked with nearby academics, focusing on outer ears for the earbud design and inner ears for the acoustics,’ she says. Thousands of ears were scanned, and only by bringing them all together did the company find the ‘design space’ to work within. ‘I think we’ve assembled one of the largest ear libraries anywhere,’ Hankey says. ‘The database is where the design starts,’ Bauerly continues, ‘and then we iterate and reiterate.’” On July 28 2021, Apple was referred to as “[an] ear-canal innovator.”141

In 2020, Apple’s patent filings describe a system for deriving biometrics using embedded biometric sensors on the AirPods (Earbuds).142 The patent captures waveforms associated with the cycling profusion of blood to the skin, so multiple biometric parameters can be collected,

---

139 The secrets behind the runaway success of Apple’s AirPods: The wireless headphones have been a surprise hit. Here’s how: Sept 5 2020, [https://www.wired.co.uk/article/apple-airpods-success](https://www.wired.co.uk/article/apple-airpods-success)
140 Inside Apple Park: first look at the design team shaping the future of tech, Dec 9 2021, [https://www.wallpaper.com/design/apple-park-behind-the-scenes-design-team-interview](https://www.wallpaper.com/design/apple-park-behind-the-scenes-design-team-interview)
141 Can you ID me now? Apple les for ear-canal biometrics patent, Jan 28, 2022., [https://www.biometricupdate.com/202201/can-you-id-me-now-apple-files-for-ear-canal-biometrics-patent](https://www.biometricupdate.com/202201/can-you-id-me-now-apple-files-for-ear-canal-biometrics-patent)
including, for example, heart rate, blood volume, and respiratory rate. Ears have been flagged as the future of biometric-based mass surveillance.

On March 4 2022 Apple (via Orrick lawyers) wrote to the U.S. federal government that:

While we still believe these reasons are pretext for Apple’s retaliation against me for reporting safety issues, discrimination, labor violations, and fraud – if Apple really thinks I violated their policies in protesting these invasive technologies, then their policies are wrong.

**Other User Studies**

Despite Apple’s censoring of employee concerns about user studies, Apple is quite public about its user studies. Just searching LinkedIn for “Apple User Study,” numerous people/positions are returned with detailed descriptions of the roles and projects. In these descriptions, Apple talked about “small, focused research studies” and “large-scale worldwide [user study] operations.” Positions talked about user studies and data collection for “sensor and health technology,” “biometric data” and for “product comfort.” Positions

---

143 Patent number 10856068
145 3D Ear Biometrics BIR BHANU, HUI CHEN, Center for Research in Intelligent Systems, University of California, Riverside, CA, USA, Springer
146 Letter from Apple Inc (via Orrick, Herrington & Sutcliffe LLP) to U.S. Department of Labor, March 4 2022, [b] PII
149 https://www.linkedin.com/jobs/view/2944349447
150 https://www.linkedin.com/jobs/view/2944349447
included responsibilities such as to “identify and recruit user study participants,”151 and “observe behavior” and “administer complex testing protocols.”152

During my time at Apple, I was invited to employee user studies looking to study me on topics ranging from my “eye movements,” “grip on an iPhone,” “voice”, “blood pressure,” physical response to “yoga, swimming, and running,” to studying my “menstruation” and “sleep.” Indeed, in April 2019 I was invited to a user study program to study my sleep.153

“Congratulations! You have been selected to participate in the official kickoff of the Sleep LiveOn program. This survey will collect a couple more pieces of information before you can sign up for a session to pick up hardware. If you have a co-sleeper participating, you may want to wait to take the survey with them in the room.” 154

Going forward, I would then be surveyed via email about my “insomnia severity index” and other medical information while a Beddit monitor155 was required to be placed under me as I slept, monitoring my heart rate, respiratory rate, and other data.156

The request for co-sleeper information also extended to requesting co-sleepers sign NDAs, and even participate in the study themselves – even if they are not an employee. Personally, I didn’t want my employer to know who I was sleeping with and I stopped participating in that study.

151 https://www.linkedin.com/jobs/view/2938135938
152 https://www.linkedin.com/jobs/view/2944353441
153 Email from LiveOn R&D to (b)(6) PII, April 1 2019, Subj: LiveOn Sleep: You’re Invited!
154 Email from LiveOn R&D to (b)(6) PII, April 1 2019, Subj: LiveOn Sleep: You’re Invited!
155 iMore, Apple cans the Beddit Sleep Monitor 5 years after buying the business, https://www.imore.com/apple-cans-bddit-sleep-monitor-5-years-after-buying-business
156 Email from LiveOn R&D to (b)(6) PII, April 16 2019, Subj: LiveOn Sleep: Insomnia Severity Index Survey
RADAR & SYSDIAGNOSE

When Apple employees file “Radar” tickets to track software development work and “bugs,” they include detailed information about the problems they are seeing. The default sharing settings for most Radar ticket included all of software engineering. Radar tickets also are not removable. Even when the tickets are closed, they remain searchable. In training, employees say they are told: “Radar is forever.” 157

When employees file Radar tickets, they are often asked to include diagnostic files, internally called “sysdiagnose” to give Apple more information about the problem. If they are filing a bug about iMessage, they might be asked to install a sysdiagnose profile that exposes their iMessages to the team tasked with fixing the issue. For employees using a live-on device, default settings can mean that, as they are filing a Radar ticket, a sysdiagnose profile is being automatically created in the background, sending data to Apple without the employee realizing it. When sysdiagnose profiles are not included, employees have been known to post memes calling out the omission. 158

I told The Verge journalist that I filed a ticket about Apple’s photo search capabilities. I was quoted as writing, 159

Radar, and many of the Radars I submitted with detailed logging and personal details were visible to tens of thousands of people.

Whether it is the text content of the Radar, or the logs attached, if a coworker wanted to learn intimate details about your life, they could by simply searching through the Radars you’ve filed. Reviewing logs quickly exposes locations, routines, friends, and other highly personal data. Assumably far more data would be made available to the Worldwide Loyalty Team.

---


(b)(6) PII
Secrecy

Secrecy Policies

The New York Times wrote in 2009 that, “Few companies are more secretive than Apple, or as punitive to those who dare violate the company’s rules on keeping tight control over information. Secrecy at Apple ... is baked into the corporate culture.” 160 Anil Dash (EFF board member and advisor to the Obama administration) wrote that Apple “chooses to operate with an extreme and excessive layer of secrecy, even when making reasonable business decisions.” 161 Dash wrote, “the cost of Apple keeping secrets has become morally and ethically untenable” and that “Apple spends an enormous amount of money on protecting and obfuscating normal business operations that any other company can do in the open.”162

A 2017 internal training video included a quote from VP of Marketing, Greg Joswiak, telling employees that “I have faith deep in my soul that if we hire smart people they’re gonna think about this, they’re gonna understand this, and ultimately they’re gonna do the right thing, and that’s to keep their mouth shut.” 163

Apple’s “New Product Security (Secrecy)” team is part of the larger Global Security team. Before joining Apple, the Global Security team manager, David Rice,164 worked at the NSA as a Global Network Vulnerability Analyst for four years, and before that was a Special Duty Cryptologist in the U.S. Navy.165 Before joining Apple, other Apple Global Security managers have worked in US Coast Guard port security,166 local Police Chiefs,167 as U.S. Secret

---

164 David Rice, https://www.linkedin.com/in/david-rice-7b3686/
166 Sean Downey, https://www.linkedin.com/in/sean-downey-64a942119/
INFORMATION FOR OSTP ON AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT IN THE UNITED STATES

Service Special Agents, U.S. Department of State Special Agents & Executive Protection managers for weapons manufacturers, etc.

In 2017, Rice complained that “U.S. employees have griped about [Apple's] draconian security measures.” With McCarthyism-flavored PSYOPs, Apple tells its employees that “leakers” at Apple “look like [regular employees],” and that “they come to work, they don’t appear any different, and they start off with the exact same motivation about ‘I love Apple, I think this is a cool place to work, I wanna make it better.’”

I had grown deeply disturbed by the horrific lack of privacy for Apple corporate employees and was happy to expose to the public, as the anti-privacy policy for employees was a “feature” not a “bug” to Apple, and thus there was no internal complaint process on the matter, and even if there was, it seemed like a certain way to face additional retaliation.

The Verge article about Apple’s work conditions saying:

- “Apple has an internal culture of surveillance, intimidation, & alienation. Employees are closely monitored & our data hoarded in the name of secrecy & quality. We’re told we have no expectation of privacy, while Apple says publicly: privacy is a human right.”
- “Apple probably considers what they’re doing to employees “internal information.” Why? For secrecy? For quality? Or because Apple knows the public would be outraged, & that outrage might start to “deprogram” their employees? “
- Cult: “great devotion to a person, idea, object, movement, or work.” Information control: “encourage spying on other members” Behavior control: “instill obedience”
- “I still love Apple products & brand. I devoted nearly 7 years & much blood/sweat/tears ensuring Apple's products are exceptional. However, Apple the corporation needs a reckoning. Apple's policy of "secrecy" should not shield it from public scrutiny about human rights & dignity.”
- “We’re learning about Apple’s long history of systemic oppression & retaliation against employees when employees express concerns about discrimination, harassment, & other

abuse. Why wouldn’t Apple try to use our data & their internal surveillance infrastructure against us?”175

Thomas le Bonniec, an ex-Apple contractor and whistleblower, wrote to regulators in 2019: “It is worrying that Apple keeps ignoring and violating fundamental rights and continues their massive collection of data. “I am extremely concerned that big tech companies are basically wiretapping entire populations despite European citizens being told the EU has one of the strongest data protection laws in the world. Passing a law is not good enough: it needs to be enforced upon privacy offenders.”176 Le Bonniec, said Apple has been, “operating on a moral and legal grey area and they have been doing this for years on a massive scale. They should be called out in every possible way.”177

Le Bonniec exposed that Siri is recording when it is not triggered by the users. Thousands of recordings were sent to Apple in order for hundreds of Apple employees to listen, analyse and transcribe their content. The public statement reveals that Apple collected millions of confidential messages, full of intimate details, political opinions, sexual preferences, and discussions between persons in a room, without the users even being aware of it. In 2019, Apple admitted that these practices were not up to the privacy standards. According recent disclosures it seems that contrary to Apple’s statement, no end was put to the recording of Apple’s users.178

In January 2023, the NLRB found merit in my charge that Apple’s NDAs do violate federal labor laws.179 There are still no decisions on my or Le Bonniec’s surveillance charges.

SEARCH AND PRIVACY POLICIES

In September of 2021, a journalist wrote about my experience realizing just how intensively Apple could and likely was surveilling me. She wrote,

---

175 (b)(6) PII
179 TechCrunch, Labor officials found that Apple execs infringed on workers’ rights, https://techcrunch.com/2023/01/30/labor-officials-found-that-apple-execs-infringed-on-workers-rights/
I told the journalist it "I told the journalist it"

In 2019, a former Apple executive also had a rude awakening and alleged that Apple reviewed his private text messages. He wrote, “To further intimidate any current Apple employee who might dare consider leaving Apple, Apple’s complaint shows that it is monitoring and examining its employees’ phone records and text messages, in a stunning and disquieting invasion of privacy.”

In 2021, I filed complaints with the U.S. NLRB and the California Dept of Labor over Apple’s unlawful employee policies, including their “Workplace and Searches Privacy.”

“In order to protect Apple confidential and sensitive information and maintain the security and integrity of our networks and equipment, any use of Apple property, as well as use of your personal devices for Apple business or for accessing Apple networks, is subject to this policy.”

---

184 Apple Inc: https://people.apple.com/US/en/subtopic/845; Photographing employees engaged in protected concerted activities constitutes unlawful surveillance because it has a tendency to intimidate employees and interfere with exercise of Section 7 rights. Photographing in the mere belief that something "might" happen is not a sufficient justification. F.W. Woolworth Co., 310 NLRB 1197 (1993); see also, National Steel and Shipbuilding Co., 324 NLRB 499 (1997) (peaceful union rallies); Labor Ready, Inc., 327 NLRB 1055 (1999), (employer videotapes of workers employed by temporary service in waiting room waiting for assignments unlawful).
185 Note: Overbroad
“Workplace Searches. Apple may: Access, search, monitor, archive, and delete Apple data stored on all of its property, as well as non-Apple property, if used for Apple business or if used for accessing Apple data, servers, or networks. This includes all data and messages sent, accessed, viewed, or stored (including those from iCloud, Messages, or other personal accounts) using Apple equipment, networks, or systems. Conduct physical, video, or electronic surveillance, search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises.”

“This means that you have no expectation of privacy when using your or someone else’s personal devices for Apple business, when using Apple systems or networks, or when on Apple premises.”

“The search or removal of Apple-related content on a device will be determined on a case-by-case basis when there is a business need and subject to local approval processes. Refusing to permit a search or removal of Apple-related content may result in disciplinary action up to and including termination of employment.”

The GDPR notes that employee monitoring may result in the collection of non-employees’ personal data. The GDPR and the BDSG also apply to the collection, processing, and use of non-employees’ personal data. Accordingly, the employer must have a valid legal basis for processing non-employees’ personal data and must notify nonemployees about potential personal data collection. Here, Apple simply tell employees they have no expectation of privacy whatsoever and makes no statements to non-employees who may get caught in Apple’s mass-surveillance infrastructure.

Apple is in a unique position, perhaps only comparable to Google & ISPs/carriers, where they have access to an incredible amount of data as system administrators of services and those services are provided by monopolies. If Apple wanted to read its employee’s personal emails, and that employee used iCloud, Apple could simply login to its own systems and read the emails. This is the same for data backed up in iCloud backups, or saved on iCloud drive, or send through iMessages. Apple owns the hardware of one of the handful of phones and computers, and even if Apple employees were to use a different company’s products, anyone they interacted with who

---

186 Boeing Corporation Advice Memo (2013). Boeing must cease and desist from creating the impression that its employees’ union and/or protected concerted activities are under surveillance. Register Guard, 344 NLRB 1142, 1144 (2005) (test is whether the employee would reasonably assume from the statement that their union activities had been placed under surveillance.” Flexsteel Industries, 311 NLRB 257, 257 (1993).
187 Note: Overbroad
188 Note: Overbroad. Do organizing and union materials count as Apple-related?
189 Employee Monitoring (Germany), Resource ID: W-008-3362, HOLGER LUTZ AND SIMONE BACH, BAKER MCKENZIE, WITH PRACTICAL LAW DATA PRIVACY ADVISOR
did use Apple’s products would give Apple a way to spy on that employee through their friends. The same is comparable for Google employees. In this sense, there is no such thing as a “personal” device for an Apple employee. That also weaponizes many consumer products if the non-employee user is simply communicating with an Apple employee on that product.

The Verge’s August privacy article:

Underpinning all of this is a stringent employment agreement that gives Apple the right to conduct extensive employee surveillance, including “physical, video, or electronic surveillance” as well as the ability to “search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises.” Apple also tells employees that they should have “no expectation of privacy when using your or someone else’s personal devices for Apple business, when using Apple systems or networks, or when on Apple premises.”

Further, I also filed charge against an email Tim Cook sent his employees on September 21 2021 responding to an employee or employees speaking with journalist about a meeting where Tim Cook talked about the pandemic, remote work, employee benefits, and pay equity.

“I want you to know that I share your frustration. These opportunities to connect as a team are really important. But they only work if we can trust that the content will stay within Apple. I want to reassure you that we are doing everything in our power to

---

190 Twitter. [b](6) PII


192 Apple Inc, Tim Cook to Apple_Employees$@group.apple.com, Date: Sept 21, 2021, Subj: Follow-up on global team meeting
Identify those who leaked.\textsuperscript{193} As you know, we do not tolerate disclosures of confidential information, whether it’s product IP or the details of a confidential meeting.\textsuperscript{194} We know that the leakers constitute a small number of people. We also know that people who leak confidential information do not belong here.\textsuperscript{195} \textsuperscript{196}\textsuperscript{197}\textsuperscript{198}

The NLRB agreed with me and found there was merit to my charge against Cook in January 2023.\textsuperscript{199} Shortly after Apple hired a prior NLRB Board Chair to defend them (Harry Johnson), and shortly after that, NLRB told me there will be a ‘re-decision’ of merit on the charge. There is no such thing as a ‘re-decision of merit’. I filed a complaint with General Counsel’s office arguing there must have been unlawful \textit{ex parte} communications by Johnson leading to the regulatory subterfuge of a ‘redecision of merit’ (avoiding settlement or adjudication), which violates the NLRA, APA, and my Due Process rights. I have not heard back from NLRB for months.

\textsuperscript{193} \textit{Register Guard}, 344 NLRB 1142, 1144 (2005) (test is whether the employee would reasonably assume from the statement that their union activities had been placed under surveillance.” \textit{Flexsteel Industries}, 311 NLRB 257, 257 (1993),
\textsuperscript{194} \textit{Report of the General Counsel Concerning Employer Rules, NLRB Memorandum GC 15-04} (2015)
\textsuperscript{195} \textit{Yale New Haven Hospital}, 309 NLRB 363, 368 (1992) (supervisor unlawfully threatened employee with reprisal by telling an employee that if he did not stop protected activities he would “talk” to him again; implies that the talk will not be mere conversation but will concern the employment of the offending employee).
\textsuperscript{196} \textit{Valerie Manor, Inc.}, 351 NLRB 1306 (2007) (threat of unspecified reprisals).
\textsuperscript{197} \textit{Equipment Trucking Co., Inc.}, 336 NLRB 277 (2001) (statement, If you don’t like it, find another job, implied threat of discharge).
\textsuperscript{198} \textit{Medco Health Solutions Of Las Vegas, Inc.}, 357 NLRB No. 25 (2011) (respondent’s statement that, if employee could not support the respondent’s policies, there were other jobs out there and perhaps “this wasn’t the place for him” was an implied threat in violation of 8(a)(1)).
\textsuperscript{199} Bloomberg, Apple Executives Violated Worker Rights, Labor Officials Say, 
Information for OSTP on Automated Worker Surveillance and Management in the United States

Public Policy

[Collecting user data] is surveillance. These stockpiles of personal data serve only to enrich the companies that collect them.
- Tim Cook (2018)

I can’t think of any other company that has so proudly, and so publicly, distributed spyware to its own devices. The only restraint is Apple’s all-too-flexible company policies.
- Edward Snowden (2021)

“Ubiquitous employer surveillance of workers has a long and rich history as a defining characteristic of workplace power dynamics, including the de facto abrogation of almost any substantive legal restraints on its use. This history can be traced through many pivotal points including massive efforts through warfare, slavery, globalization, and other forms of colonialism used to control and exploit workers. What is novel, and of real concern to privacy law, is that rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace - bleeding into the private lives of employees.”

There are areas of an employee's life in which his employer has no legitimate interest.

“The protection of workers' privacy is a civil rights issue: both for the protection of human dignity rights and because privacy invasions can serve as vehicles for unlawful discrimination. History has shown that economic pressures are an unreliable regulator for the preservation of the civil rights of those with comparatively lower economic power. We cannot simply look to the market to curtail abuses of power regarding worker surveillance.”

---

The predominant view of the U.S. Courts is that consent is not effective if it is not freely
and voluntarily given. The protection for privacy & autonomy is a default rule that recognizes
a sphere of protection, not only to protect civic and personal life, but also to mirror the likely
implicit bargain between the employer and employee about where the employment relationship
ends and personal life begins. Even in the context of initial employment, consent to a
particular type of invasion does not mean consent to all varieties of that invasion,
reasonable or unreasonable.

The employer also cannot discharge employees for refusing to waive a nonnegotiable or
nonwaivable right. When an employee successfully refuses to submit to an employer's
wrongful intrusion into protected employee privacy interests and the employee suffers a
termination of employment or such adverse conditions of employment as to amount to a
constructive discharge because of the employee's refusal to submit, the employee has a claim for
wrongful discharge in violation of public policy. The public policy is the protection against
wrongful employer intrusions into protected employee privacy interests.

However, companies may be able to process personal data if they obtain either subjects'
voluntary affirmative consent to process data for the specific purpose intended or have a
legitimate justification. Corporations in countries such as Germany and France tend not to rely
on consent because employees must be expressly asked for it, must be able to refuse without risk
of sanction, and can withdraw it at any time. Moreover, in the corporate investigation context,
courts tend to assume that such consent is involuntary because of the imbalance of power between
the employer and employee.

U.S. organizations that control or process the personal data of European Union residents
likely are subject to the EU’s new data protection requirements, the General Data Protection

206 See Stores, Inc. v. Lee, 74 S.W.3d 634, 647 (Ark. 2002); Papa Gino's of America, Inc., 780 F.2d 1067, 1072 (1st
Cir. 1986) (applying New Hampshire law; employee contracted away certain rights by accepting employment from
employer who forbade drug use, but employer's demand that employee submit to polygraph exceeded scope of
employee's consent to allow reasonable investigation into drug use).
207 Restatement of the Law, Employment Law § 7.03, Protected Employee Privacy Interests in the Employee's
Physical Person and in Physical and Electronic Locations, Comments
209 Restatement of the Law, Employment Law > Chapter 7- Employee Privacy and Autonomy
§ 7.07, Discharge in Retaliation for Refusing Privacy Invasion, Comment
210 Restatement of the Law, Employment Law > Chapter 7- Employee Privacy and Autonomy
§ 7.07, Discharge in Retaliation for Refusing Privacy Invasion, Comment
211 ARTICLE: THE LAW OF CORPORATE INVESTIGATIONS AND THE GLOBAL EXPANSION OF
CORPORATE CRIMINAL ENFORCEMENT, 93 S. Cal. L. Rev. 697 May 2020
Regulation (GDPR). A common practice in the U.S. is to rely on blanket consent clauses in employment contracts or handbooks that permit employers to process employee personal data. U.S. employers often also rely on implied consent from employees. However, such practices may not be considered valid forms of consent for lawful processing of personal data under the GDPR. The GDPR provides that consent must be “freely given, specific, informed and unambiguous.” Moreover, the GDPR adds, consent is not “freely given” where a “clear imbalance of power” between the data controller (i.e., employer) and the data subject (i.e., employee) exists.\(^{212}\)

The Article 29 Working Party emphasized the imbalance of power in the employment context: “Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.” The Working Party also advises that the imbalance of power in the employment relationship makes voluntary consent questionable and, for most work-related data processing, the GDPR lawful basis relied upon “cannot and should not” be the employee’s consent.\(^{213}\)

Multiple GDPR factors invaliding employee to employer consent are present with Apple’s user studies. First, when I responded to the initial email about the Gobbler user study, I had no idea what I consented to/initiated, as it was “vague or unclear.” Next, I had no “clear records to demonstrate they consented,” as no receipt was sent and I was never given a copy of the ICF. It appears Apple also no longer has a copy of the ICF, otherwise it seems they would have provided it to me on Sept 15 or quoted it in their position statement.

Next, there was “a clear imbalance of power between [the employer] and the individual,” the “employee would be penalized for refusing consent,” and “there was no genuine free choice over whether to opt in.” Between the general pressure for Apple R&D employees to “live on” new products and software, and to participate in studies, and my performance reviews

---

\(^{212}\) Is Employee Consent under EU Data Protection Regulation Possible?, Joseph J. Lazzarotti and Maya Atrakchi, February 27, 2018

\(^{213}\) Is Employee Consent under EU Data Protection Regulation Possible?, Joseph J. Lazzarotti and Maya Atrakchi, February 27, 2018
I

NFORMATION FOR

OSTP ON AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT IN THE UNITED STATES

mentioning my participation in these programs, but also that barbed wire compound with armed guards, too.

Finally, apparently later some employees were given the option to use the Gobbler application but not be “whitelisted” so their PII would not be uploaded. However, I was not given this option nor even told it was an option, so “consent was a precondition of a service, but the processing is not necessary for that service.” Finally, once I apparently signed the ICF and after the Gobbler app was installed on my phone, I had no way to disable the app, nor was I given any way to withdraw consent. I had talked to other employees about the app with similar concerns over the years. Thus, the “consent” was invalid because Apple “did not tell people about their right to withdraw consent” and “people cannot easily withdraw consent.”

This non-consensual user data harvesting doesn’t only have implications on Apple’s employees and their families and friends. Intellectual Property rights cannot be granted for unlawful things/acts. Apple has deployed technology across the world, based on arguably illegal data and the fruit (algorithms and features) grown from that illegal data. What rights does Apple actually have to their technology if the people the data was harvested from had their own rights violated? What does that mean for customers using Apple products built off of human rights violations (again)? Today, the success of the global economy depends on Apple’s success. Apple cannot take these kind of risks when the fall-out may land everywhere.

Apple says privacy is a fundamental right and “fundamental rights should not differ depending on where you live in the world.” Apple says, “they treat any data that relates to an identified or identifiable individual or that is linked or linkable to them by Apple as ‘personal data,’ no matter where the individual lives.”

California courts have found, "The constitutional [privacy] provision is self-executing; hence, it confers a judicial right of action on all Californians. Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone.”

California accords privacy the constitutional status of an inalienable right, on a par with defending life and possessing property.

214 Information Commissioner’s Office Consultation: GDPR consent guidance Start date: 2 March 2017 End date: 31 March 2017


217 Vinson v. Superior Court (1987) 43 Cal. 3d 833, 841 [239 Cal. Rptr. 292, 740 P.2d 404] [limiting right to discover one’s sexual history, habits and practices in action for sexual harassment and emotional distress].

986
Apple is headquartered in California. Article I, section 1 of the California Constitution provides that the right of "privacy" is among the people's inalienable rights. California appellate courts and at least one federal court have consistently held, in varying contexts, that Article I, section 1 provides some protection against non-governmental intrusion, as well as state conduct.\(^{218}\) The legislative history (ballot argument) stated,

"The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us."\(^{219}\)

California employees have a cause of action against their private employer for violating their Constitutional right to privacy if the intrusion is against a legally protected privacy interest, including: "conducting personal activities without observation, intrusion, or interference" as determined by "established social norms."\(^{220}\) While California employees could contractually agree not to assert a right to privacy, the employer cannot be allowed to use such an agreement to circumvent the public policy favoring privacy, and the employer could not successfully enforce such a contractual agreement if it intruded on plaintiff's right to privacy.\(^{221}\) The public policy here "affects the duty not to intrude on the right of privacy, which inures to the benefit of the public at large rather than to a particular employer or employee."\(^{222}\)

California employees have the right to privacy, even at the workplace, in areas where there is a reasonable expectation of being left alone. For example, the California Labor Code prohibits video or audio monitoring of employees in restrooms, showers, locker rooms, and dressing rooms.\(^{223}\) Further, California Penal Code section 647j makes it a crime for a person


\(^{220}\) *Hill*, 7 Cal.4th 1, 35, 26 Cal.Rptr.2d 834, 865 P.2d 633.

\(^{221}\) *Foley v. Interactive Data Corp.*, 47 Cal.3d at p. 670 (1988)

\(^{222}\) *Semore v. Pool* (1990) 217 Cal. App. 3d 1088

\(^{223}\) California Labor Code § 435, Contracts and Applications for Employment; § 435 was enacted to clarify "privacy rights in the workplace for both employers and employees" since court decisions had "left a definite gray area in regards to employee surveillance." Hearing on A.B. 2303 Before the Assemb. Comm. on Labor & Emp't, 1997-98
unlawfully to invade someone else’s privacy via a device to view in a private room, or by secret recording or photograph of a person’s body.  

At a federal level, under the National Labor Relations Act (NLRA), employers may not monitor or surveil employees participating in protected concerted activities, including “creating the impression of surveillance.” Further, 18 U.S.C. § 1801 makes it a federal crime to capture images of a private area of an individual (naked or undergarment clad genitals, pubic area, buttocks, or female breast) without their consent and to knowingly do so under circumstances in which the individual has a reasonable expectation of privacy.

While the legislative history for federal labor laws probably never anticipated a mega-corporation using a tool they called the “Face Gobbler” to capture secret videos of employees 24/7 – one would think The Congress would be outraged by an employer, one that markets that “privacy is a human right” none the less – justifying the termination of an employee who already had an open NLRB charge against the employer – on the employee protesting invasions of privacy & Gobbling of their face.


224 California Penal Code Section 647(j) PC, Criminal Invasion of Privacy in California,


Conclusion

No matter what it says, Apple is not a company committed to data privacy. Apple’s business model helped stimulate the data-privacy dystopia we now occupy. Apple is allowing the surveillance-capitalism atrocities it claims to oppose.


It’s clear Apple’s use of surveillance and electronic monitoring in the workplace is illegal, unlawful, and otherwise unethical. It’s clear Apple knows this.

The Restatement makes clear: information regarding an employer's illegal activities is not a trade secret.228 Further, information regarding an employer's illegal activities is not protectable by means of restrictive covenant. 229 The public policy protecting whistleblowers would be completely thwarted if the employer could retaliate with impunity against any employee who decided to reveal improper conduct by the employer.230

Yet, Apple is notorious for oppressing & silencing their workforce. An opinion piece was written by Anil Dash about the issue. Dash is “recognized as one of the most prominent voices advocating for a more humane, inclusive & ethical technology industry,” was an advisor to the Obama White House, and is a Board Member of the EFF (Electronic Frontier Foundation) an international, non-profit digital rights group.231 Dash wrote about Apple:

The sad truth is that Apple is still stuck in an anachronistic, 1984 mode of communicating with the world. If Apple doesn’t evolve, it’ll become a pathetic-looking giant, constantly playing whack-a-mole with information leaks, diminishing its relevance by antagonizing the very creators it has so long sought to identify with. … The reckoning Apple has reached, whether it’s admitted or not, is that its secrecy is compromising its humanity…It’s incumbent upon Apple to do the moral thing here. Treat your employees, customers, suppliers and partner companies better, by letting them participate in the thing most of your products are designed for: Human self-expression. If the ethical argument is unpersuasive, then focus on the long-term viability of your marketing and branding efforts, and realize that a technology company that is determined to

228 Restatement of the Law, Employment Law, § 8.02, Definition of Employer's Trade Secret, Comment
229 Restatement of the Law, Employment Law, § 8.02, Definition of Employer's Trade Secret, Comment
231 EFF, Anil Dash, https://www.eff.org/about/staff/anil-dash
prevent information from being spread is an organization at war with itself. Civil wars are expensive, have no winners, and incur lots of casualties.\(^{232}\)

Apple clearly did not listen.

The US government has not taken this seriously either. Both the NLRB and US Dept of Labor initially responded to my charges by attempting to intimidate me to withdraw those charges, and then when I refused, attempting to intimidate me and interfere with my due process rights. NLRB is now supposedly investigating. US Dept of Labor has only escalated it animosity towards me. California Dept of Labor says it won’t even start investigating for another 1-3 years. Meanwhile I’m now unemployed, denylisted, broke, in debt, severely ostracized, & my reputation destroyed by smears and defamation.

What is the point of ‘worker protection laws’ or ‘privacy ‘laws’ if they are never enforced? Do we live in a democracy if corporations are above the law? The first step here is not passing new laws or enacting more MOUs; the first step is deciding that no company is above the law. The first step is ensuring labor agencies will actually fulfill their statutory obligations. We must all agree that labor rights are human rights, and human rights must be protected.

Please let me know if I can be of any help. I’m more than happy to provide documents, testimony, or other additional resources. Thank you.

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0196
Comment on FR Doc # 2023 12995

Submitter Information

Email: [REDACTED]
Organization: Public Citizen

General Comment

Please see attached comments of Public Citizen.

Attachments

Public Citizen Comment - RFI Automated Worker Surveillance and Management 6.29.2023
Comment of Public Citizen to the White House Office of Science and Technology

Request for Information: Automated Worker Surveillance and Management

Docket Number OSTP-FRDOC-0001

On behalf of Public Citizen’s 500,000 members and supporters, we thank the White House Office of Science and Technology (“Office”) for working to ensure automated surveillance systems do not undermine workers’ rights, opportunities, access, health or safety.

Public Citizen stands for the right of people to live their lives without undue interference from corporate power, and for putting power back where it belongs — in the hands of human beings.

It is impossible to live a life in the modern world free from commercial surveillance. The connected world has brought benefits, but those benefits have come with costs. We therefore again commend the Office on starting the valuable process of categorizing the harms of surveillance in the workplace, and even more importantly beginning to rebalance power in favor of workers rather employers who seek to use surveillance that endangers the health and safety of workers.

Workers Need Protections Against the Abuse of Surveillance by Employers (Question 1)

Oversight of employee performance is an integral aspect of managing a productive workforce. However, there is an important distinction between supervising effective performance of workers and abuse of technology to patrol all employee activities. Data collection tactics developed in the consumer realm are now being used by employers to assert control over the workplace and, in turn, control over workers.1 Unfortunately, the adoption of invasive and exploitative workplace surveillance is being normalized, with eight out of 10 of the largest employers in the U.S. digitally monitoring their employees.2 It’s a practice that degrades the rights, privacy, health and safety of workers.

Employees may not know how they are being tracked and what information is being collected about them. It can include sensitive information and a security breach that reveals the worker data raises the same privacy concerns and damage risk as a security breach of customer

information. Additionally, some employers use information acquired from data brokers to make hiring decisions, yet “[a]lgorithmic decisions made based on these data points can easily become proxies for discrimination and bias.” Others employ surveillance to chill worker collective organizing.\(^5\)

Invasive surveillance systems create a harmful work environment. The lack of transparency in data collection also puts workers at an extreme informational disadvantage, increasing corporate power and decreasing the bargaining power of the labor force.\(^6\) The imbalance gives employers the control to exploit workers, particularly vulnerable and marginalized populations, even using opaque data collection to engage in wage theft.\(^7\) Workers must submit to unfair and deleterious workplace practices in order to put food on their tables.

*Surveillance of Workers Has Increased Dramatically*

There is a long history of aggressive scrutiny of workers, and even the use of investigative services to gather information on employees.\(^9\) However, that level of surveillance was used sparingly because it is both expensive and time consuming.\(^10\)

As technology has quickly advanced, so have the options for monitoring the actions of employees both inside and outside the workplace.\(^11\) The use of closed-circuit television cameras and key cards that track employee entrance and exit from the workplace have graduated to body cameras and GPS trackers. A Wisconsin tech company started an optional program that implants microchips in employees.\(^12\) Despite dubious scientific validity and racial and sexist bias,\(^13\) facial tracking and voice recognition software is being used to scrutinize public-facing workers to ensure they are using appropriate facial expressions and vocal tone with customers.\(^14\) Bio-tracking, though still in early development, can be a useful worker protection tool to identify dangerous changes in heart rate, body temperature, kidney function and other physiological

---

3 Andrea Miller, *More Companies Are Using Technology to Monitor Employees, Sparking Privacy Concerns*, ABC News (March 10, 2018), [hereinafter Miller, More Companies Are Using Technology to Monitor Employees.].
4 Adler-Bell and Miller, *How Surveillance and Capitalism Are Shaping Workers Future*.
5 See, e.g., Jo Constantz, ‘They Were Spying On Us’: Amazon, Walmart, Use Surveillance Technology To Bust Unions, *NEWSWEEK* (December 13, 2021), [hereinafter Hanley and Hubbard, AMAZON’S SURVEILLANCE INFRASTRUCTURE AND REVITALIZING WORKER POWER, OPEN MARKETS INSTITUTE, (September 1, 2020), [hereinafter Hanley and Hubbard, AMAZON’S SURVEILLANCE STRUCTURE,].
6 Adler-Bell and Miller, *How Surveillance and Capitalism Are Shaping Workers Future*.
7 Id.
8 KATHRYN ZICKUHR, **WORKPLACE SURVEILLANCE IS BECOMING THE NEW NORMAL FOR U.S. WORKERS**, WASHINGTON CENTER FOR EQUITABLE GROWTH (August 18, 2021), [hereinafter ZICKUHR, WORKPLACE SURVEILLANCE IS BECOMING THE NEW NORMAL.]
9 ZICKUHR, **WORKPLACE SURVEILLANCE IS BECOMING THE NEW NORMAL**.
10 Id.
11 This includes surveillance of contract workers, as well as surveillance of franchise workers by corporate headquarters. Id.
14 See, e.g., ZICKUHR, **WORKPLACE SURVEILLANCE IS BECOMING THE NEW NORMAL**.
factors. However, employers are also spuriously attempting to use it to measure worker emotion and mood, a presumptive proxy for worker productivity.\footnote{Emine Saner, \textit{Employers Are Monitoring Computers, Toilet Breaks – Even Emotions. Is Your Boss Watching You?}, \textit{The Guardian} (May 14, 2018), \url{http://bit.ly/3EA6xMe}.
}

An explosion of digital monitoring unfolded as more of the workforce began working from home. Use of surveillance software dramatically increased with the COVID-19 pandemic.\footnote{Jennifer Alsever, \textit{Your Company Could Be Spying On You: Surveillance Software Use Up Over 50% Since Pandemic Started}, \textit{Fortune} (September 1, 2021), \url{http://bit.ly/3OcqzQc}.
}

Technological systems available to employers include software giving employers access to private worker messages on Slack, “attention tracking” on Zoom videoconferencing,\footnote{Public outcry against the ZOOM’s monitoring software caused the company to disable the feature. \textit{See}, Eric S. Yuan, \textit{A Message to Our Users}, ZOOM BLOG (April 1, 2020), \url{http://bit.ly/3E9UNyI}.

Microsoft Office 365 software allows employers to track worker activity in great detail without notifying a worker that they are being tracked.\footnote{Rachel Sandler, \textit{Microsoft’s New Productivity Score Lets Your Boss Monitor How Often You Use Email and Attend Video Meetings}, \textit{Forbes} (November 25, 2020), \url{http://bit.ly/3UK80Wb}. Though Microsoft modified the software to aggregate worker data in response to public pushback, research shows that the program continues to allow employers to collect extensive data on individual workers. Bill Goodwin, \textit{Microsoft Office 365 Has Ability To Spy On Workers}, \textit{Computer Weekly} (June 21, 2022), \url{http://bit.ly/3Gv3yGe}.
} In a recent survey, 78% of employers acknowledged the use of monitoring software to track employees and 73% reported evaluating employee performance and/or making decisions to terminate employees using stored worker emails, calls and videos. Yet, 83% of employers in the same survey admitted that this type of data collection is ethically questionable.\footnote{Mark C. Perna, \textit{Why 78% Of Employers Are Sacrificing Employee Trust BySpying On Them}, \textit{Forbes} (March 15, 2022), \url{http://bit.ly/31xeZG1}.

\textit{Worker Surveillance Offers Limited Benefit to Employers}

Surveillance technologies can be useful in guarding against theft, unsafe work practices and workplace violence. While these purposes are often cited by employers, concerns about productivity are the primary reason given for use of most technological surveillance systems. However, many types of surveillance and the manner in which they are used belie this rationale. For example, many employers utilize technology to furtively monitor and record workers without notifying workers that they are doing so. In these cases, decisions about the worker — including salary, promotions, discipline and termination — are made based on information the worker did not know was being collected or used. By failing to use collected data to provide workers with appropriate feedback, there is no opportunity to improve job performance or increase their productivity.

Even when workers are aware of surveillance by the employer, workplace productivity may not improve. In fact, it may reduce worker performance by increasing mistakes and causing workers focus on quantified behavioral metrics that may not reflect tasks necessary for successful
completion of job goals. Surveillance also creates an environment of distrust between workers and management, causing a disconnect that hampers worker loyalty and accountability. Research has shown that, in some cases, monitored workers may be more likely to disregard instructions, work at a slower pace, and even steal from the company. Creating zones of privacy for workers, on the other hand, has been shown to increase performance.

The newfound ease of inexpensively collecting information on employees has led many employers to engage in intensive oversight through surveillance of almost every aspect of a worker’s activities. This level of data collection is impossible for employers to analyze. Therefore, they turn to algorithms that fail to effectively capture worker performance — focusing on specific actions rather than outcomes. By relying on these algorithms to determine worker pay or direct disciplinary actions, employers betray the rights of employees and make arbitrary, unprofitable business decisions.

**Intense Scrutiny is a Weapon to Control Workers**

Unfortunately, the adoption of invasive and exploitative workplace surveillance is being normalized and employers are increasingly operating with a “Big Brother” mentality.

Amazon warehouses, for example, use sensors and tablets to monitor workers’ movements, tracking how many boxes they’ve filled. Amazon uses its package scanners not only to track packages, but also to measure the number of seconds between each scan made by a worker. One worker reported that the established quota required her to scan one item every 11 seconds (300 items per hour). Workers who fail to reach their quotas may be reprimanded or fired. The breakneck pace of the work can cause repetitive stress injuries. Also, workers feel pressured to ignore safety precautions in order to keep up, increasing the chances of workplace harm.

---

26 *Zickuhr, Workplace Surveillance Is Becoming the New Normal.*
28 *Zickuhr, Workplace Surveillance Is Becoming the New Normal.*
29 Id.
30 Hanley and Hubbard, *Amazon’s Surveillance Structure.*
32 Id.
33 Id.
accidents.\textsuperscript{34} Indeed, inspectors with the Washington Department of Labor and Industries cited a direct connection between the pressure to work at high speed and worker injuries at an Amazon delivery station.\textsuperscript{35}

Sometimes the procedures for monitoring can be the direct cause of an injury. FedEx workers have experienced intense, persistent pain from the repetitive stress of moving boxes with a heavy package scanner strapped to their forearm.\textsuperscript{36}

As part of its Global Smart Logistics Network,\textsuperscript{37} UPS trucks have become a rolling computer filled with hundreds of sensors that track every aspect of the worker and truck movements, such as when the engine is turned on, if the truck is backing up, when the door is open, and whether a seat belt is buckled.\textsuperscript{38} The handheld computer used to gather customer signatures is also a GPS monitor.\textsuperscript{39} It prescribes turn-by-turn directions and tracks when delivery drivers exceed time limits for each package delivery.\textsuperscript{40} UPS guidance, sometimes called “The 340 Methods,” includes everything from which shirt pocket to stow their pen to how to occupy their time on an elevator.\textsuperscript{41}

Surveillance practices that monitor workers every minute place intense scrutiny on any time not being used to accomplish work tasks. Workers feel forced to work through pain and injuries.\textsuperscript{42} The system pressures workers to limit rest and bathroom breaks.\textsuperscript{43} UPS drivers, for example, have to account for Stops Per On-Road Hour, forcing them to justify bathroom breaks.\textsuperscript{44} Not surprisingly, UPS drivers and workers at other companies that enforce minute-by-minute accountability report limiting their bathroom breaks.\textsuperscript{45} This puts the health of the worker at risk and can increase workplace accidents due to worker distraction. Additionally, rest breaks are essential to avoid health risks to workers, including heat-related illness.\textsuperscript{46}

\textsuperscript{34} Id.
\textsuperscript{35} Will Evans, \emph{Amazon’s Warehouse Quotas Have Been Injuring Workers for Years. Now Officials Are Taking Action}, REVEAL (May 15, 2022), \url{http://bit.ly/3OkEzaH}.
\textsuperscript{36} Jessica Bruder, \emph{These Workers Have a New Demand: Stop Watching Us}, THE NATION (May 27, 2015), \url{http://bit.ly/3hOiGbA} [hereinafter Bruder, \emph{Stop Watching Us}].
\textsuperscript{37} See, UPS Deploys Purpose-Built Navigation For UPS Service Personnel, UPS (December 4, 2018), \url{http://bit.ly/3UJRWn6}.
\textsuperscript{39} Goldstein and Chase, \emph{The Future of Work}.
\textsuperscript{40} Id.: \emph{UPS Deploys Purpose-Built Navigation For UPS Service Personnel}, UPS (December 4, 2018), \url{http://bit.ly/3UJRWn6}.
\textsuperscript{41} Bruder, \emph{Stop Watching Us}.
\textsuperscript{42} Evans, \emph{Ruthless Quotas at Amazon}.
\textsuperscript{43} See, e.g., ZICKUHR, \emph{WORKPLACE SURVEILLANCE IS BECOMING THE NEW NORMAL}; Evans, \emph{Ruthless Quotas at Amazon}; Conley, \emph{Strict Rules}; Hanley and Hubbard, \emph{AMAZON’S SURVEILLANCE STRUCTURE}.
\textsuperscript{44} Bruder, \emph{Stop Watching Us}.
\textsuperscript{45} See, e.g., ZICKUHR, \emph{WORKPLACE SURVEILLANCE IS BECOMING THE NEW NORMAL}; Evans, \emph{Ruthless Quotas at Amazon}; Bruder, \emph{Stop Watching Us}; Emine Saner, \emph{Employers Are Monitoring Computers, Toilet Breaks – Even Emotions. Is Your Boss Watching You?}, THE GUARDIAN (May 14, 2018), \url{http://bit.ly/3EA6xMe}.
\textsuperscript{46} See, e.g., Juley Fulcher, \emph{BOILING POINT: OSHA MUST ACT IMMEDIATELY TO PROTECT WORKERS FROM DEADLY TEMPERATURES}, PUBLIC CITIZEN (June 2022), \url{https://www.citizen.org/article/boiling-point/}. 

\url{https://www.citizen.org/article/boiling-point/}. 

\url{https://www.citizen.org/article/boiling-point/}. 

\url{https://www.citizen.org/article/boiling-point/}. 

\url{https://www.citizen.org/article/boiling-point/}. 

\url{https://www.citizen.org/article/boiling-point/}. 

\url{https://www.citizen.org/article/boiling-point/}.
Workplace Surveillance Damages the Mental Health of Workers

The stress of constant surveillance creates a serious problem for the mental health of workers. Often the perception of workers is that they are under coercive surveillance with an eye toward finding people to fire. In a study of TSA agents under surveillance using closed circuit television, one officer described the surveillance system as managers “looking for excuses to slap you on the hand.” A UPS driver said, “It’s like you’re fighting for your job every day.” And a report on Amazon’s use of surveillance described the relationship between the company and its employees as one of “control, humiliation and unabating anxiety.”

Michael Childers, the director of the University of Wisconsin’s School for Workers called this type of surveillance activity “management by stress.” He described the anxiety and exhaustion of workers at a call center where every conversation and keystroke was monitored, “You had 20-year employees quitting, people throwing up in the parking lot.” Such surveillance can create a “constant low-grade panic” that seeps into a worker’s private time and even invades their sleep. The deterioration of mental and physical health caused by this stress is compounded by the increased risk of injury as a worker’s ability to function is compromised.

Workers Risk Losing Their Jobs for Reporting Dangerous Employee Practices

Employers often retaliate against workers who report improper employer practices through discipline, demotions, reduced hours, termination and interference with attempts to gain alternative employment. The fear of retaliation is a powerful deterrent for employees who cannot afford to lose their livelihood, leaving the door open for unrestrained exploitation of workers. Any attempts to hold employers accountable for abusive and dangerous surveillance practices are undermined if those in a position to identify it are unable to come forward.

It is only through effective protection of employees from retaliation that abusive worker surveillance practices can be identified and stopped. Such protection includes education of employees on their rights and easy access to a responsive complaint system. Importantly, the employee must be able to access relief swiftly. Delays leave workers suffering emotionally and financially while they wait for agency action. In addition, slow investigations allow employers to continue unacceptable employment practices, leading to the continued harm of workers. Any policy placing limits on the use of surveillance practices must, of necessity, include whistleblower protections for workers.

47 Antebay and Chan, Why Monitoring Employees’ Behavior Can Backfire.
48 Morrison, Just Because You’re Working From Home Doesn’t Mean Your Boss Isn’t Watching You
49 Antebay and Chan, Why Monitoring Employees’ Behavior Can Backfire.
50 Bruder, Stop Watching Us.
51 Hanley and Hubbard, Amazon’s Surveillance Structure.
52 Bruder, Stop Watching Us.
53 Id.
54 See, e.g., Hanley and Hubbard, Amazon’s Surveillance Structure.
Concentrated markets and the growing dominance of large employers have seen wages of the average worker stagnate while the salaries of top executive soar.\textsuperscript{55} The imbalance has allowed employers to capitalize on the absence of regulations on the use of surveillance technologies to exploit workers at the expense of worker rights, privacy, safety and health.\textsuperscript{56} With worker power eroded, it is necessary for OSHA to step in and provide oversight protection to workers.

For the reasons outlined above, a rule limiting the use of surveillance practices must include the following protections for workers:

1) Employers should be prohibited from invasive surveillance of workers, including the capture and/or use of information without a clear and valid business purpose that outweighs the privacy and safety risks to employees.

2) Employers should be prohibited from selling, sharing or transferring any surveillance data collected on employees to third parties and limitations should be placed on the length of time data can be stored.

3) Employers should be required to disclose surveillance practices to workers, including what information is collected, how it is collected, how long it will be retained, who has access to it, and how it will be used.

4) The Office should work in concert with OSHA to protect workers from surveillance practices that expose workers to a risk of physical or psychological harm.

5) An OSHA rule should delineate strong, unambiguous protections of workers from retaliation by employers for reporting abusive or dangerous surveillance practices or violations of consumer privacy. The anti-retaliation protections must include a clear enforcement mechanism through the OSHA Whistleblower Office\textsuperscript{57} and the option to seek redress in the courts if worker claims cannot be investigated in a timely manner.

Conclusion

The erosion of our autonomy through invasion of our privacy in and out of the workplace is not minor or imaginary, nor is privacy correctly imagined as lurking under some kind of nebulous constitutional shadow.\textsuperscript{58} The rights, and the harms, are concrete. Privacy rights are civil rights.\textsuperscript{59}

\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} The OSHA Whistleblower Office enforces 25 whistleblower statutes. See, https://www whistleblowers.gov.
\textsuperscript{58} Griswold v. Connecticut, 381 U.S. 479 (1965) at 481-86.
They are human rights. Workers rights are human rights. And in the corporate surveillance economy, they are violated every day.

*The White House Office of Science and Technology* has a chance to take a decisive step toward rebalancing power in favor of workers and to ensure they do not have to trade their health and safety for their livelihoods. We applaud the Office for doing this important work, and look forward to engaging further as the process goes forward.

Thank you for the opportunity to comment on this significant worker health and safety issue. For questions, please contact Juley Fulcher, worker health and safety advocate in Public Citizen’s Congress Watch division, at [redacted].

---

PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0197
Comment on FR Doc # 2023 12995

Submitter Information

Email: [email protected]
Organization: Jobs With Justice

General Comment

See attached file(s)

Attachments

JWJ RFI on Worksite Surveillance June 29th
Jobs With Justice believes that all workers should have collective bargaining rights, employment security, and a decent standard of living within an economy that works for everyone. We are a national coalition that brings together labor, community, student, and faith voices at the national and local levels to win improvements in people’s lives. Over the past couple of years, Jobs With Justice has joined frontline workers at Amazon and begun working with various allies and stakeholders seeking to support these workers to improve the conditions within one of the largest, most profitable companies in human history. We know that due to the enormity of Amazon as an employer, the company’s use of automated surveillance and management of workers is not only illustrative but influential throughout the economy. If we do not set standards for Amazon, then they are poised to set standards for everyone else in ways that threaten collective bargaining and employment security.

Jobs with Justice has been supporting and learning from Amazon workers in a variety of ways, and have heard stories that point to a trend in how technology is used to monitor and manage workers seriously threatens workers’ rights – workers know they are being tracked but don’t know how the information is being used, creating anxiety or fear that ultimately interferes with workers' right to organize.

Amazon workers from Massachusetts to Arizona have reached out to our local groups to look for support after they have burnt out by the harsh conditions or have become injured on the job, a phenomenon spurred on by electronic surveillance. For example, our Arizona chapter helped fundraise for a worker who became injured. She had talked to supervisors about her back problems but did not think it registered. What did register, however, was her performance and she quit her job because she could not keep up with the expectations around metrics generated by the wearable devices. Jobs With Justice has seen in many industries that health and safety complaints or other issues raised by workers take time to be elevated by supervisors or get to the right person in management. But workers at Amazon are getting cut off before their issues are properly dealt with or before they can organize to make the company improve.

In a recent conversation with Philadelphia Jobs With Justice, a worker leader from an area warehouse shared that they are always aware of the being monitored, but they do not
understand how much data is collected, how it is stored, or how the metrics are calculated. They are constantly reminded of the monitoring by the messages they receive on their devices. The messages are mostly about rates. They shared that they were aware of co-workers who have been punished for poor performance, whereby supervisors show metrics from the device, but they don’t understand the standards that are being applied to the data that is being collected. This plays into Amazon’s hands, exacerbating the imbalance of power between workers and their employer.

We have also heard from ongoing conversations with warehouse workers and community organizers from Bessemer, Alabama, how pernicious automated surveillance can be to mental health and the psyche of workers. This has been reinforced by a report by Rutgers University and Michigan State professors, Amazon’s Policing Power: A Snapshot from Bessemer1 where they found, unfortunately and unsurprisingly given the historical nature and generational trauma related to the control of Black workers, that surveillance harms Black workers in even harsher ways:

“The testimony before the NLRB also provided a snapshot of how it feels to be a Black worker at Amazon's Bessemer fulfillment center: isolated and hyper-surveilled under the constant presence of private security and off-duty police officers. Highlighting the Bessemer case as part of an ongoing nationwide study, this report brings a racial lens to the numerous ways Amazon polices its workers, particularly through the use of private security and arrangements with local police. These types of worker control tactics create a culture of intimidation for all workers, but the consequences are amplified for Black workers, particularly in the southern United States. Amazon's approach in Bessemer is marked by a stark convergence of racialized economic exploitation and racialized policing with long historical roots in the Black Belt and beyond.” (p 1)

In our most recent efforts to understand the conditions inside Amazon warehouses and provide workers with information about their rights to organize and improve their jobs we have been reaching out to former warehouse workers in the New York area. These conversations have reinforced that even former workers remember vividly the experience working at Amazon and the negative impacts on their health. One former employee stated, "I just felt like a body being used to lift heavy things." and after raising their concerns consistently with Amazon they walked off the job after being berated by a manager about work pace. Several workers described similar issues with lifting heavy objects and feeling constant pressure to perform from management to the point of having to quit.

Workers are under constant stress to meet rates and know their every moment is monitored. We have heard how workers are dehumanized, working through pain and injury to meet productivity demands. The surveillance does not take into account past injuries and recovery or provide leniency. Mental health problems are pervasive and workers have cited surveillance’s negative

---

impact on their mental health. Surveillance also intensifies feelings of worker precarity – automated warnings and terminations without input from supervisors.

The seriousness of fear and anxiety and the impact of this monitoring of workers can be seen in the findings in a report authored by Daniel Hanley and Sally Hubbard, titled “Eyes Everywhere: Amazon’s Surveillance Infrastructure and Revitalizing Worker Power” which explains how worker surveillance endangers the mental and physical health of Amazon workers. This report establishes how surveillance enables Amazon to deter workers from unionizing, increases the precarity of workers who can be terminated at any time for deviating from metrics they don’t even know exist, and leads to other dominant firms adopting similar practices.

Fear and anxiety induced by surveillance create real barriers to worker organizing. We know Amazon uses its surveillance infrastructure to impede worker organizing. Amazon extrapolates internal and external variables to determine unionizing risk through things such as heat maps and poverty and diversity indexes. Amazon tracks workers’ activities and alters the production line (slowdowns) or uses supervisors on the floor to discourage and impede workers from engaging with one another. Even moving employees to less traffic areas if they’re suspected of organizing.

In conclusion, we believe there to be real negative mental and health consequences related to automated surveillance that ultimately hurt workers’ ability to exercise their rights and organize to improve their jobs. Given Amazon’s track record of exploitation and union busting, it should be considered by this and future investigations how the effects of monitoring and automated management hurts workers’ rights and any regulatory or enforcement solutions must specifically address how to protect workers’ fundamental right to organize. We have an opportunity to set standards in evolving industries, standards that will shape the climate for worker participation and industrial democracy for the foreseeable future. The courageous workers leading the fights within Amazon deserve better, starting with the elimination of surveillance that insights fear and creates barriers to organizing. This is not simply a struggle against the abuse of technology that threatens workers’ rights. It’s the struggle to achieve an era of dignity, respect, and democracy for all of us.

Nafisah Ula, Organizing Director, Jobs With Justice Education Fund

Pallavi Rao, Coalition Organizer and Strategic Researcher, Philadelphia Jobs with Justice

2 https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffe823958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf (accessed 6/26/23)
General Comment

Please see attached letter from Service Employees International Union.

Attachments

SEIU OSTP automated worker surveillance comment - June 2023
June 26, 2023

Alan Mislove, Assistant Director for Data and Democracy  
Office of Science and Technology Policy  
Executive Office of the President  
Eisenhower Executive Office Building  
1650 Pennsylvania Avenue  
Washington, DC 20504

RE: Request for Information; Automated Worker Surveillance and Management; Docket ID OSTP-TECH-2023-0004

To whom it may concern:

The Service Employees International Union (SEIU) submits this letter in response to the White House Office of Science and Technology Policy’s (OSTP) Request for Information on Automated Worker Surveillance and Management. SEIU is a union that represents over two million working people in health care, the public sector, and in other service and care jobs as homecare workers, child care providers, janitors, security guards, and airport workers. We strive to ensure that every worker has a living wage, benefits to support their family and dignity in retirement, and safe, equitable workplaces where all employees meaningfully participate in the decisions affecting their employment. This comment supplements the letter we sent to your office in January 2022 in response to OSTP’s previous request for input on a “Bill of Rights for an Automated Society”.

Our previous letter highlighted the risks of surveillance, faulty algorithms, legal violations, wage theft, and work intensification that come packaged with automated technologies. This letter illustrates those harms through examples from our members and organizing campaigns.

---

1 Office of Science and Technology Policy, “Request for Information; Automated Worker Surveillance and Management”, https://www.regulations.gov/docket/OSTP-TECH-2023-0004
I. Surveillance to interfere with labor rights: Starbucks Corporation

Employers use surveillance technology to worsen an already unequal power relationship between themselves and individual workers. Workplace surveillance and data collection generate large amounts of data on workers that employers often use to discriminate against or punish workers. They even use it as a weapon to interfere with workers’ legal right to organize their workplaces.

Workers at a Starbucks store in Memphis were trying to organize a union through Workers United, an SEIU affiliate. The company used remote video surveillance to identify certain employees who had been engaged in union activities. It used that same video surveillance to accuse these workers of company policy violations and then fire them. But the workers allege that the supposed violations were commonplace practices at the store and that Starbucks’ anti-union animus was the real reason for the firings. Court proceedings that followed these illegal firings brought to light that Starbucks conducts comprehensive remote video surveillance of workers in its stores.

A Senior Manager at Starbucks testified in court, “The Genetec [Clearance] system is a -- it's a housing system, or it's a security system where I and other folks can remotely view live events in the store as well as past history events in the store. So it's literally a camera system there… They're running 24 hours a day, seven days a week… cameras placed throughout the entire store.” He admitted using the surveillance footage to identify certain workers who had been engaged in union activities in the workplace, and whom Starbucks accused of the policy violations.

Unions and collective bargaining enable workers to reclaim their social and economic power. There is direct and immediate economic injury for workers who lose their jobs because of illegal retaliation. And when the right to organize a workplace is threatened, it not only harms the individual worker, but also their colleagues and the labor movement as a whole. McDonald’s and Amazon have similarly used surveillance to illegally deter or retaliate against workers attempting to organize.

---

6 Id.
II. Commodification of intellectual property through video recordings: California College of the Arts and Notre Dame de Namur University

The pandemic compelled workers in higher education to switch to remote learning, which meant faculty started posting their syllabuses, reading materials, assignments, and lectures to digital platforms managed by colleges and universities. SEIU Local 1021 in Northern California represents public sector and nonprofit workers including adjunct faculty at California College of the Arts and Notre Dame de Namur University.

Instructors at these and many colleges are required to upload their lectures to school-run servers. Sometimes existing curriculum is given to a lecturer to use, but often the lecturer creates the course and its curriculum from scratch for the school. The ownership of this digital content is ambiguous. Concordia University in Canada, in an egregious example, ran a class using recorded lectures of a professor that had passed away years earlier. This issue is further complicated because when schools acquire debt, they list assets including intellectual property as collateral. If schools default on their loans, then the liquidated assets under the lenders’ possession would include the work product created by faculty.

Course material, especially lecture videos and slides, should belong to the person who created them. Adjunct faculty lack job security, and the curriculum and scholarship they create is hyper-specific to their careers. Having control and ownership over their work is how academic workers find jobs and build careers. That the school owns the means of distribution should not entitle these institutions for use of the work product in perpetuity. Scholars should have a say on whether their course materials can be reused and be able to set the terms on how much they’re compensated for it.

III. Use of phone apps with geotracking features: janitorial services

SEIU Local 32BJ represents workers in the cleaning industry. Many janitorial services employers require that their workers download apps on their personal phones. This presumably helps workers with human resource functions such as clocking in and out of shifts without needing to touch a time clock. But these apps collect much more information than simple timecards might. They have geolocation and geotracking features that let employers log the worker’s location at certain intervals. Many employers use geofencing that limits geolocation to when the worker is within building premises, but less sophisticated employers may not instill this feature. Sometimes employers propose using the apps to make workers clock in throughout their shifts, tracking their movements minute-by-minute. Because these workers are represented by a union, we have successfully been able to push back against unreasonable surveillance.


10 Paycorp, Paychex, Team lighthouse software application, and proprietary software such as SBM employer management platform are some examples of these apps.
Reliance on smartphones leaves behind workers who do not own such expensive phones, or who are unfamiliar or uncomfortable using this technology while still perfectly adept at completing their work tasks. Even if a worker has a smartphone and is comfortable using it, if they accidentally damage their phone or forget to bring it to work, they would have to scramble for alternatives. Making timecard features digital mainly only benefits employers. Digitization likely means paychecks may only be available online, which makes it difficult for many workers to access them or prove pay violations.

Certain problems arise with relying on this type of app technology that do not exist in analog (paper timecard) systems. Contracted cleaning workers clean buildings belonging to third parties—for example, office buildings—that sometimes do not have strong wireless signals. If work time isn’t properly logged because of signal issues, that creates the room for noncompliance with wage and hour laws. Above all, being compelled to download apps with geotracking capabilities makes workers feel their personal device and privacy is invaded.

IV. Algorithms managing rideshare drivers: Uber and Lyft

SEIU Locals have been supporting rideshare drivers who are organizing through Drivers Demand Justice and California Gig Workers Union to demand better pay and working conditions.

Rideshare drivers interact with a management system that is entirely through apps on their personal phones. The Uber and Lyft apps are how drivers get work. They know the drivers’ location, know when they’re driving, monitor all their work, evaluate the feedback they receive from passengers, and calculate their pay. Drivers have no interaction with a human other than their passengers.

The app-based technology used by gig companies has the effect of exerting substantial control over workers through pay incentives and ratings systems, but at the same time Uber and Lyft misclassify their drivers as independent contractors. Through this misclassification, the companies disclaim any employment relationship with the workers and save on labor costs by ignoring their obligations regarding minimum wage and overtime pay, unemployment insurance, payroll taxes, and workers’ compensation.11

Lack of pay transparency

Pay is unilaterally determined by Uber and Lyft algorithms. The driver never knows what the passenger is paying for a ride and what portion of it is funneled to the corporation.12 Researchers analyzed data from New York City, which has a minimum pay rate for drivers; in other words, likely the best scenario for rideshare drivers in the country.13 They found companies took at least

30 percent of the passenger fare in about a third of the rides. They also found passenger fares are going up over time at a steeper rate than increases in driver pay.

Drivers incur substantial expenses, including insurance, maintenance and repair costs, depreciation, fuel, and payroll taxes. But the pay is piecework and erratic. This inconsistency hurts drivers’ ability to plan or predict what they might earn during a given shift, leaving them financially precarious and vulnerable.

Threat of deactivation exposes workers to unsafe situations

If passengers complain or issue low ratings, Uber and Lyft temporarily or permanently deactivate the app for drivers.\textsuperscript{14} Deactivation has serious consequences as it cuts workers off from their livelihoods. And there is no due process by which the worker can challenge these decisions.

This has resulted in drivers accepting rides and tolerating passenger behavior that jeopardizes their safety and wellbeing. And the experience is considerably worse for drivers of color.\textsuperscript{15} A national safety survey of rideshare drivers found that two-thirds of respondents “were threatened, harassed, or assaulted in the last year”.\textsuperscript{16} Of these drivers, “52 percent said they were verbally abused, 40 percent said they experienced damage to their vehicle, and 32 percent said they were called a racial, ethnic, or religious slur. Drivers also reported being sexually propositioned (27 percent), threatened with physical harm (26 percent), and grabbed, groped, or hit (14 percent).”\textsuperscript{17}

The fear of low ratings and deactivation disincentivizes drivers from rejecting rides that make them feel unsafe. Fifty-nine percent of drivers who took on unsafe rides “did so because they were concerned about negative reviews leading to deactivation. For drivers of color, this rate was seventy percent.”\textsuperscript{18} Seventy-two percent of drivers of color reported “experiencing some type of threatening, harassing, or violent behavior… with 86 percent reporting being called a racial, ethnic, or religious name or slur.”\textsuperscript{19}

This has terrible consequences. Between 2017-2021, 121 Uber drivers and 101 Lyft drivers were targeted in carjackings, 28 rideshare and app-delivery drivers were killed, more were severely or permanently injured, and many of the victims were immigrants, women, or elderly.\textsuperscript{20}

\textsuperscript{16} Id.
\textsuperscript{17} Kristin Toussaint, “More than two-thirds of rideshare drivers have been threatened, harassed, or assaulted”, Fast Company, https://www.fastcompany.com/90884204/more-than-two-thirds-of-rideshare-drivers-have-been-threatened-harassed-or-assaulted
\textsuperscript{19} Kristin Toussaint, “More than two-thirds of rideshare drivers have been threatened, harassed, or assaulted”, Fast Company, https://www.fastcompany.com/90884204/more-than-two-thirds-of-rideshare-drivers-have-been-threatened-harassed-or-assaulted
\textsuperscript{20} Dara Kerr, “More Than 350 Gig Workers Carjacked, 28 Killed, Over the Last Five Years”, The Markup, https://themarkup.org/working-for-an-algorithm/2022/07/28/more-than-350-gig-workers-carjacked-28-killed-over-
figures are likely an undercount. Uber has produced at least “24,000 safety incident reports . . . involving physical assaults against Uber Drivers by Riders” from 2017 to 2020, according to a plaintiff’s filing in a federal lawsuit against the company.21

V. Conclusion

In sharing these examples of automated surveillance and management, we would like to point out that we don’t have a complete understanding of how pervasive these technologies are or all the ways they’re affecting workers. This is because employers aren’t obligated to disclose the surveillance they conduct on workers or how they use that data, so workers are in the dark about the full extent of these practices. Until employers are obliged to disclose their methods, the true picture of what is happening to workers will remain incomplete. Moreover, these examples stem from existing technologies; technology is evolving so rapidly that potential for impacts will be even greater as we move forward in time.

We hope to see your office work to restrain the abusive use of worker surveillance and algorithmic management technologies against workers. The concerns we have raised are within unionized workplaces, which do not represent the majority of workers in America. Our siblings in other sectors of the economy and in nonunionized workplaces have been subject to even worse abuses.

Advancement in surveillance and automation technologies has created inhumane working conditions that jeopardize workers’ rights, autonomy, privacy, and even their safety. Workers have gained very little from the proliferation of these technologies which are used to control and manipulate them under the guise of ensuring productivity and convenience. Workers are happier and more productive when they have autonomy and some control and flexibility over their work lives. Increasing company profits at the price of workers’ humanity is not a bargain worth making.

Thank you for this opportunity to share our perspective. Please don’t hesitate to contact me if you have any questions.

Sincerely,

Sowmya Kypa
Senior Policy Analyst
Service Employees International Union

---

General Comment

See attached file(s)

Attachments

2023.06.29 TJ Workplace Surveillance Comments
June 29, 2023

Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

RE: Comment on Request for Information on Automated Worker Surveillance and Management

Thank you for the opportunity to comment on the widespread harms caused by using automated tools to surveil and control workers. Absent aggressive action across several agencies of the federal government, the “future of work” risks becoming a future of algorithmic manipulation and surveillance that will strip workers of dignity, power, and voice, suppress wages, and exacerbate our nationwide workplace health and safety crisis. Marginalized communities and workers of color will suffer the most. The Consumer Financial Protection Bureau (CFPB), Equal Employment Opportunity Commission (EEOC), Federal Trade Commission (FTC), Department of Justice (DOJ), Department of Labor (DOL), National Labor Relations Board (NLRB), and the Occupational Safety and Health Administration (OSHA) should act urgently and in concert to address this evolving threat to workers.

Towards Justice is a nonprofit legal organization that uses impact litigation, policy advocacy, and collaboration with workers and workers’ organizations to build worker power and advance economic justice. These comments are informed by our ongoing engagement with workers and our litigation and advocacy on behalf of workers suffering from surveillance and algorithmic control. Examples of our advocacy in this space include litigation on behalf of rideshare drivers in California alleging that Uber and Lyft cannot on the one hand deny them labor rights while on the other hand use algorithms to manipulate and control them, including by setting the prices charged to consumers, without violating California antitrust and unfair competition laws.1 We also represent Amazon delivery drivers alleging that Amazon—in part through the use of invasive worker surveillance tactics—denies drivers reasonable access to the

bathroom and creates an illegal disparate impact on people with typically female anatomy. We have also represented workers in a variety of cases challenging unfair competition in the labor market, and in cases combatting the misuse of big data to harm low-wage workers. Meanwhile, we have engaged in extensive advocacy on behalf of workers harmed by employer-driven debt, including earned wage access products that may allow employers to obtain extensive information about the financial circumstances of their workers. Because harm to workers often implicates several areas of law, we strive to provide de-siloed advocacy support to our clients and often help workers and worker organizations to use labor standards laws, competition laws, and consumer protection laws to level the playing field and build worker power.

Employers have always kept tabs on worker behavior and performance and have always sought to manipulate and control workers while evading legal responsibilities to them. But in the past two decades, employers have increasingly sought to exploit technologies that allow them to obtain even more granular and real-time information about workers and to manipulate and control workers by hidden algorithms. Modern workplace surveillance is used to track productivity; monitoring the number of packages a warehouse worker scans per minute or the number of keystrokes a desk worker completes on her computer. It is used to keep tabs on worker location, eye movement, internet browsing, and electronic communications. “Now, with the advent of almost ubiquitous network records, browser history retention, phone apps, and the like, it is getting very difficult to hide your activity.”

electronic sensors, wearable fitness trackers, thermal sensors, and facial recognition systems, there truly could be limitless worker surveillance.”

Real-time surveillance of workers is often coupled with real-time control of workers whether through human managers or algorithms that can exploit detailed information about workers to manipulate their behavior and depress their wages. Because these forms of control—although often more invasive and coercive than control exercised by human bosses—are hidden some companies (especially in the so-called “gig economy”) have attempted to argue that they can exercise control over workers in this way without being accountable to them under the labor laws. In this way, workplace surveillance and algorithmic control are inextricably intertwined with misclassification.

These systems dramatically reduce worker autonomy, undermine fair competition, and disparately impact protected classes of workers in ways that reinforce historic marginalization. In addition, these technologies are often implemented without worker knowledge, and usually without full disclosure of what is being tracked, what the goalposts are, or what the consequences are if goals are not met. And once data about workers is collected, workers have limited ability to access that information or to protect it from inappropriate use or disclosure. This creates a general environment of fear that modifies worker behavior in concerning ways. It can encourage workers to work far beyond expected productivity goals, while chilling both collective action and enforcement of workplace rights.

These extensive harms cannot be resolved by one agency of government. In fact, worker surveillance and algorithmic control are often exploited by employers in an attempt to skate between various legal regimes. Control by hidden algorithm alongside misclassification, for example, may seek to evade the authority of the DOL or NLRB, but in doing so, implicate the authority of the CF PB, DOJ, and FTC. The primary goal of these comments is to highlight the authority of the CFPB, DOL, DOJ, EEOC, FTC, NLRB, and OSHA and emphasize the need for aggressive and coordinated action across the federal government to address these challenges. The comments include some specific recommendations, but they also raise many unanswered questions, questions that can only be resolved if the federal government is acting in concert to address these harms.

1. The Federal Trade Commission and Department of Justice

Employers’ use of workplace surveillance and the related automated management of workers implicates antitrust and competition laws and laws prohibiting unfair and deceptive acts and practices within the jurisdiction of the FTC and the DOJ.

---

While competition laws regulating conduct involving multiple firms may not apply directly to employers’ exercise of workplace surveillance and automated management over employees within the firm, firms that classify their workers as independent contractors are subject to such regulations when they use surveillance technologies and algorithms to exercise control over workers that are purportedly outside the firm. The so-called gig economy provides a clear example. The use of surveillance and algorithmic control to engage in “wage discrimination” and set prices charged to customers at optimal amounts for the companies, provides powerful evidence of the control that app-based delivery and rideshare companies exercise over their drivers—evidence relevant to the question whether the companies owe those drivers labor rights. But if those workers are properly classified as independent contractors, then their use of surveillance and automated management in these ways implicate antitrust and competition laws governing vertical price restraints and wage and price discrimination. Even if such conduct does not violate the Sherman or Clayton Acts in some circumstances, the FTC has highlighted how such conduct may be an unfair method of competition under Section 5 of the FTC Act.

Gig companies often also use surveillance and algorithmic management technologies to develop pay models that can make it impossible for workers to make ends meet unless they work exclusively for a single company, thus effectively preventing workers from moving between employers. Again, these payment models are powerful evidence of misclassification, but they can also be understood as restraints on worker mobility that may violate antitrust and unfair competition laws, especially when coupled with the companies’ extensive market power. Put bluntly, the gig companies cannot have it both ways. They cannot deny workers labor rights without the control they exercise over those workers being subject to laws governing vertical restraints and unfair competition.

Workplace surveillance across purportedly independent firms may implicate unfair competition and antitrust laws even when workers are properly classified as employees. This may arise where powerful firms seek to use labor market intermediaries to avoid accountability to workers while simultaneously exercising control over workers and the intermediary firms. For example, Amazon’s extensive surveillance of its delivery drivers, which it claims not to employ, and who are employed directly by Amazon’s Delivery Service Partners (DSPs), is powerful evidence that Amazon in fact employs those workers. But surveillance also exacerbates the
vertical restraints that Amazon exercises over its DSPs. It is much harder for DSPs to provide services to firms besides Amazon when Amazon’s surveillance and management technology has constant eyes on DSPs and delivery drivers—including through video cameras inside DSP vans. As a consequence, Amazon DSPs may be captive to Amazon, which can exploit its market power to set prices and wages in ways that undermine worker bargaining power.¹⁴

Together, the FTC’s unfair method of competition authority and its unfair and deceptive act and practices (UDAP) authority can be used to attack the ways in which worker surveillance and algorithmic management can deceive and manipulate workers. The Commission’s 2021 case against Amazon for misappropriating driver tips provides a blueprint. The FTC explained how Amazon “mislead its drivers and conceal[ed] its theft,” which made it “less likely that drivers would seek better opportunities elsewhere, helping Amazon attract and retain workers in its quest to dominate.”¹⁵ Unfortunately, “[u]nder its status quo approach, the FTC [did] not seek civil penalties for this type of abuse.”¹⁶ The agency should use all its authority under Section 5 of the FTC Act and all the tools at its disposal to attack the ways in which workers are harmed by worker surveillance and algorithmic management and control.

2. Occupational Safety and Health Administration (OSHA)

Living in a proverbial panopticon with the constant threat and possibility not only of surveillance, but of losing your livelihood if you fail to meet unknown standards, creates extraordinary physical and mental strain for many workers. This is particularly so as technology makes surveillance easier and cheaper for employers. Much thoughtful work has been done to document the physical and mental health impacts of workplace surveillance. We know that the need to meet efficiency goals—known and unknown to the worker—encourages workers to push themselves in ways that too often result in injury. Amazon’s injury rates, driven by minute-by-minute tracking of warehouse workers, have become particularly infamous.¹⁷

Pervasive workplace monitoring has had disturbing implications for workers’ ability to take care of basic bodily functions. In a report from The New York Times, “workers across a variety of jobs—pharmaceutical assistants, insurance underwriters, employees of e-commerce companies—. . . said productivity pressure had led to problems with bathroom breaks.”¹⁸ Towards Justice is now litigating a case in which Amazon delivery drivers allege that invasive

¹⁶ Id. at 2 n.12.
monitoring by Amazon forced them to pee in bottles or defecate in bags to meet their metrics.\textsuperscript{19} Even in the at-home work context, metrics requiring workers to answer phone calls within a certain number of seconds, move their mouse with particular frequency, or meet keystroke goals can keep workers tied to their desks. At Towards Justice, we met with a worker who was so constrained by at-home monitoring that she peed herself in her own bedroom because she couldn’t get up from her desk.

Such dystopian examples underscore the health impacts of workplace surveillance, as well as the extraordinary imbalance of power in the modern workplace. In workplaces where employers do not extensively surveil and manipulate workers, workers are more likely to be able to work at a healthy and safe pace and meet basic bodily functions like accessing the bathroom. But as more and more workers are governed by technologies that strip them of autonomy, we should ensure that OSHA has the resources and support to use regulation, guidance, and aggressive enforcement under the general duty provision\textsuperscript{20} to protect workers.

3. \textbf{The National Labor Relations Board}

The decline in unionization over the last half century has undermined workers’ ability to negotiate and combat invasive surveillance and monitoring. And now, constant surveillance can effectively deter or prevent unionization and other collective action.\textsuperscript{21} Pace of work requirements keep workers too busy to engage with one another. Knowing they are being watched chills worker behavior and makes them fear retaliation. Surveillance technology can be used to spread workers out or otherwise reduce opportunities for collective action. And technology can help employers identify workers suspected of or engaged in organizing.\textsuperscript{22} Although electronic micromanagement may inspire workers to fight back, and “[s]ome of the most closely monitored employees in the country have become some of the most restive”,\textsuperscript{23} it still “seems unimaginable that unlimited employer scrutiny of employees’ collective action could be consistent with the core of the National Labor Relations Act’s (NLRA’s) protections.”\textsuperscript{24}

It is crucial to safeguard workers from unlawful retaliation based on information gathered through workplace surveillance as well as employer surveillance of non-workplace activities. For example, during the COVID-19 pandemic, a Colorado-based paramedic participated in an interview for public radio that explained some of the workplace difficulties medical care

\textsuperscript{19} Matt Bloom, \textit{Amazon Delivery Drivers in Colorado Pee in Bottles, Pooped in Bags to Keep Jobs, Lawsuit Says}, Colorado Public Radio, May 23, 2023, \url{https://www.cpr.org/2023/05/23/amazon-lawsuit-delivery-drivers-quotas/}.
\textsuperscript{20} 29 U.S.C. § 654, 5(a) and (b).
\textsuperscript{23} Kantor and Sundaram, \textit{supra} n. 18.
\textsuperscript{24} Garden, \textit{supra} n. 21.
professionals faced during the pandemic. The paramedic’s employer immediately reprimanded him even though he was off duty and speaking about the terms and conditions of employment that undeniably impacted his coworkers.25

The National Labor Relations Board (NLRB) should use regulation and case decision-making to guide employers about how the NLRA constrains workplace surveillance. This guidance must reflect the challenges created by corporate coupling of labor market fissuring—the offloading of the costs and liabilities inherent to being an employer—with the simultaneous use of surveillance technologies designed to ensure corporate control over workers.26 As General Counsel Jennifer Abruzzo explained, these changes in workplace organization require a “new framework for protecting employees from intrusive or abusive forms of electronic monitoring and automated management that interfere with Section 7 activity.”27

4. The Consumer Financial Protection Board

The Consumer Financial Protection Board (CFPB) has an important role to play in protecting workers against the inappropriate use of their personal data.28 We appreciate the CFPB’s scrutiny of data brokers that obtain information about consumers through workplace surveillance.29 In 2019, Towards Justice represented a class of workers concerned that careless data sharing by a large background check services company was limiting their job prospects in violation of the Fair Credit Reporting Act (FCRA), and in 2021, Towards Justice represented clients alleging that use of criminal history on background checks to automatically bar drivers from a rideshare app ran afoul of New York’s Fair Chance Act. As the CFPB has articulated, the FCRA is not only relevant to the use of background checks in employment decisions, but also to combating unauthorized or inappropriate use of data gathered about workers. Both the dissemination of inaccurate information, and the misuse of accurate information, may constitute a violation.

Additionally, the increased use of consumer financial products and services within the employment relationship—an issue clearly within the CFPB’s authority—creates new forms of worker surveillance and automated management. Through our own litigation and advocacy, we

have seen how employers operating as creditors can exploit their power to exercise even more control over workers.30

Furthermore, employers may exploit financial information about workers obtained through their role as creditors providing employer-driven debt to further exploit and control those workers. As just one example, rideshare companies offer workers earned wage access products that may allow “early” access to wages. For example, Uber’s “Instant Pay” service allows drivers to immediately claim earnings from each ride, although they must pay a fee, ranging from $2.99 to $4.99.31 Uber of course knows how often a driver uses Instant Pay, which may offer insight into that worker’s financial desperation. Can Uber access that information when deciding how much to pay that worker? That is, can Uber add that information to the algorithm that determines worker pay and engages in so-called “wage discrimination”32 in order to pay more desperate workers less? Because the gig companies keep their algorithms hidden, it is not clear whether information gathered through consumer-creditor relationships may be used to control and manipulate workers, but this is a question that falls within the CFPB’s jurisdiction.

5. The Equal Employment Opportunity Commission

Our antidiscrimination laws (including Title VII of the U.S. Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Equal Pay Act, and the Americans with Disabilities Act) prohibit discrimination on the basis of race, color, religion, sex, national origin, age, or disability. These laws not only protect against intentional discrimination based on protected characteristics, but also against policies or practices that have a disparate impact on protected groups. The Equal Employment Opportunity Commission should aggressively combat workplace surveillance techniques and data usage policies that harm marginalized communities.

Our anti-discrimination laws should already bar the use of workplace surveillance tools to purposefully discriminate. But further clarification could help protect workers from the use of invasive technologies to find out about individual protected characteristics, even where the purposes of worker surveillance are general or opaque. For example, can a facially neutral wellness program gather information about worker health that reveals their ethnicity – like genetic information unique to individuals of Ashkenazi Jewish descent? Or that reveals health conditions unique to members of our trans community? If so, having gathered that information, how may an employer use it?

30 See e.g., Seligman Testimony, supra n. 5; see also, Dave Jamieson, When This Pilot Quit Her Job, Her Employer Billed Her $20,000, Huffington Post, Jan. 21, 2023, https://www.huffpost.com/entry/ameriflight-pilot-training-repayment-provisions_n_63a2214ee4b04414304bc464#:~:text=When%20This%20Pilot%20Quit%20Her,soon%20came%20to%20regret%20it; Taylor Telford, PetSmart offered free training. But it saddled employees with debt., Wash. Post, Aug. 4, 2022, https://www.washingtonpost.com/business/2022/08/04/petsmart-dog-grooming-training-labor-lawsuit/.
32 Dubal, supra n. 9.
Our anti-discrimination laws also should already bar the use of workplace surveillance that has a disparate impact on protected groups. For example, Towards Justice’s clients allege that Amazon’s monitoring and automated delivery performance metrics has a disparate impact on workers with typically female anatomy. In essence, by refusing to allow adequate bathroom access, Amazon has transformed urinating in a bottle into a job requirement, thus making it much more difficult for anyone who cannot easily urinate in a bottle to do the job.

The disparate impacts of surveillance may arise in other contexts as well. Pace of work requirements may inadequately accommodate disabled workers. Incorporating consumer ratings into worker surveillance—a common practice among rideshare companies and chain restaurants—may become a vehicle for consumer bias that disparately impacts traditionally marginalized workers. And worker surveillance combined with other problematic practices—like algorithmic wage discrimination—may cause a disparate impact, like the known gender disparity in earnings among Uber drivers. Finally, the hiring algorithms used by many employers—although marketed to reduce intrinsic bias—may cause discriminatory outcomes.

Our anti-discrimination laws also protect workers from hostile work environments. Constant monitoring or fear of people watching you could create a hostile work environment based on gender or gender identity. Or the fact that “[l]ow-wage workers are traditionally more likely to be surveilled, and workers of color and immigrants are most likely to be working in many of the low-wage jobs with immediate and severe consequences of surveillance,” could create a hostile work environment for these protected classes of workers.

To ensure our anti-discrimination laws can be brought to bear in these instances, we must consider the relationship between the worker and the employer, and between the surveillance technology provider and both the hiring entity and the worker. Our laws must ensure that companies that exert power over workers do not achieve free reign to discriminate against them by modifying or re-naming the employment relationship. Similarly, our laws must not exempt

surveillance technology providers from repercussions for knowingly perpetuating systemic bias regardless of the relationship they purport to maintain with either employers or workers.38

The Equal Employment Opportunity Commission should take on each of these fights, first to clarify the law and then to enforce it vigorously to prevent the perpetuation of systemic bias in the modern workplace.

6. The Department of Labor Wage and Hour Division

Workplace surveillance and control also implicates the wage and hour laws. First, it is critical that the Department of Labor address misclassification by employers that exploit workplace surveillance to control and manipulate workers, especially via hidden algorithm, while also seeking to avoid accountability to those workers under the minimum wage and overtime laws.39

Workplace surveillance also raises distinct challenges for properly classified employees that may implicate wage and hour protections. For example, a time tracking software that rounds worker time to the nearest 15-minute interval, or automatically accounts for mandated breaks, could result in time shaving in violation of wage and hour protections.40 Worker surveillance that extends beyond the temporal confines of assigned working hours also raises challenging questions: Can you be off duty while being surveilled? Or is all time when a worker is surveilled compensable work time? Meanwhile, the blending of public and private personas on social media raises new questions about compensable work. Under what circumstances does posting on a personal profile become compensable work?

Also, the DOL should consider the extent to which employers who profit off the information gathered from workers have violated anti-kickback provisions by taking a thing of value from workers that belongs to workers and exploiting it for the employer's own profits.41 The DOL Wage and Hour Division should be on the cutting edge of defining and addressing these challenges to ensure that workplace surveillance does not become a tool for cheating workers out of legally earned wages.

39 See discussion of worker misclassification in Section 1, above.
41 29 CFR § 531.35.
7. The White House Office of Science and Technology Policy

The White House Office of Science and Technology Policy is uniquely positioned to bring agency leaders together to define a proactive, de-siloed approach to the extraordinary increase in workplace surveillance and automated management. Traditionally, competition, workplace health and safety, labor relations, anti-discrimination, wage and hour, and privacy laws have been viewed as separate spheres that address separate problems and provide separate solutions. But worker surveillance blurs these lines, and we must ensure a coordinated response to this new challenge.

The White House should convene representatives of the FTC, DOJ, NLRB, CFPB, DOL (OSHA and Wage and Hour), and EEOC to develop a coordinated response to the exponential increase in worker surveillance and monitoring in the marketplace. This type of coordinated oversight is essential in an economy where the imbalance of power between workers and hiring entities is so skewed.

This response should include agency-level rulemaking to clarify how relevant legal frameworks constrain the use of worker surveillance and joint enforcement. We also recommend that the federal government require review of worker surveillance plans and affirmative disclosure of such plans to workers. Workers should know how they are being surveilled, what metrics their performance is measured against, what data is collected, who can access it, and how it is used. Workers should also have access to their own data. This effort could take a cue from the draft Worker Privacy Act developed by the Center on Privacy & Technology at Georgetown Law\footnote{Gabrielle Rejouis, \textit{A Solution to Extensive Workplace Surveillance}, Center on Privacy & Technology at Georgetown Law, Nov. 7, 2019, \url{https://medium.com/center-on-privacy-technology/a-solution-to-extensive-workplace-surveillance-8f5ab4e28b4d}.} and New York’s worker surveillance disclosure requirements\footnote{\textit{New York Employers Required to Notify Employees of Electronic Monitoring}, National Law Review, May 5, 2022, \url{https://www.natlawreview.com/article/new-york-employers-required-to-notify-employees-electronic-monitoring}.}.

At the end of the day, workers do not care if their problems are characterized as antitrust violations, discrimination, health and safety concerns, or some other label. What matters is that the government is there to police abuses of corporate power that make work stressful, invasive, hostile, unhealthy, and demoralizing. Our government must protect workers not only from employers, but from all the powerful entities that impose the threat of surveillance on workers in ways that undermine competition, endanger privacy, cause injury, and chill the exercise of workplace rights.
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0200
Comment on FR Doc # 2023 12995

Submitter Information

Email: email@email.com
Organization: National Nurses United

General Comment

See attached file(s)

Attachments

2023 OSTP_FRDOC_0001 RFI AWSM National Nurses United Comments

Attachment 1 Examples of Imaging Technology Capabilities Provided to National Nurses United by Management

Attachment 2 NNU 2021 Clinical Algorithms Final Survey Results

Attachment 3 NNU Medicare Hospital At Home Report

Attachment 4 NNU Comments AHRQ Clinical Algorithms Introduce Racial Ethnic Bias Into Healthcare Delivery
NNU knows that clinical algorithms can interfere with safe, therapeutic health care that meets the needs of each individual patient. Even under optimal conditions, clinical algorithms are based on population-level data and are not appropriate for every patient. In addition, the way clinical algorithms are implemented, regardless of how they are created, often inappropriately constrains the use of health care professionals’ judgment, which can worsen the impact of a biased algorithm.

Clinical algorithms should serve as guidelines, but employers often require rigid adherence with the goal of controlling costs and eliminating variation in treatment. First, a lower cost treatment may not be the best option. Second, health care corporations’ focus on eliminating variation aims to facilitate automation and the use of less costly labor, as individualized care requires professional judgment by skilled clinicians. Yet patients are diverse, with unique needs and values. Thus, NNU believes that decisions on patient care should be made by skilled clinicians using their professional judgment in a manner that is consistent with an individual patient’s preferences and in the patient’s best interests. Moreover, health care professionals must have the autonomy to override clinical algorithms, within their scope of practice, and not be constrained by mandates established in a corporate boardroom. Finally, NNU supports mandates for transparency as well as user and patient education on the risks associated with clinical algorithms.

NNU urges AHRQ to address several essential points that apply to all algorithms, not just those that have already been proven to be biased, as it conducts its inquiry into how clinical algorithms can introduce racial and ethnic bias into health care delivery. First, there are fundamental limits on the ability of algorithms to meet the needs of individual patients, especially when those patients are part of racial or ethnic groups that are less well represented in the data. Second, AHRQ must consider the importance of ensuring that health care professionals have full autonomy to override algorithmic recommendations, within their scope of practice and consistent with their patients’ needs and preferences. Third, transparency and education about all aspects of the creation, use, and impact of these algorithms is necessary to detect and combat bias. Fourth, transparency must extend to clinicians, patients, and the public, including thresholds for recommendations to provide and deny preventive, diagnostic, or treatment measures by race, ethnicity, gender, and other relevant data. Finally, NNU urges AHRQ to support robust regulation of clinical algorithms as medical devices and to ensure that the supporting evidence and reasoning on which clinical recommendations are based are sufficient, sound, transparent, and intelligible and that recommendation thresholds for providing or denying preventive, diagnostic, or treatment measures are transparent to clinicians, patients, and the public.

1 For example, doctors at a California hospital contend that the system to which the hospital belongs has standardized clinical guidelines through a shared electronic health record system that are “often driven by cost considerations” and that the guidelines “often conflict with their own judgment of best medical practices.” Wolfson, BJ. Orange County Hospital Seeks Divorce From Large Catholic Health System. Kaiser Health News. https://khn.org/news/article/orange-county-hospital-seeks-divorce-from-large-catholic-health-system/. Published April 13, 2012. Accessed May 1, 2021.
These comments have five main sections. Section I discusses problems related to algorithms based on clinical practice guidelines developed by experts. Section II discusses problems related to algorithms developed through machine learning. As part of the response to this RFI, NNU also has included preliminary results of our survey of RNs on their experiences with racial bias in clinical algorithms, which are detailed in Sections III and IV of these comments. Section V offers concluding recommendations.

I. Algorithms based on clinical practice guidelines developed by experts

Answering RFI question 1 on the estimated impact of these algorithms on quality of care, clinical outcomes, quality of life, and health disparities and RFI question 6 on the mechanisms by which use of algorithms contribute to poor care for Black, Indigenous, and other people of color.

A. Algorithms based on clinical practice guidelines rely on population level data that may be inappropriate for individual patients or subgroups, introducing opportunities for structural racial bias to influence health care delivery.

Clinical algorithms rely on population level data that does not reflect each individual patient’s needs and can introduce bias into health care, if clinicians are pressured to apply clinical algorithm recommendations to all patients despite individual care needs. Practice guidelines are typically based on studies and data regarding a certain percentage of a patient population as a whole and, thus, may not be appropriate for a particular patient. This is the nature of statistics: a treatment that works in a high percentage of a population is considered high-quality care. The trick, of course, is in determining where an individual patient falls relative to the population as a whole.

Patients have a range of individual factors that influence how well a particular treatment plan works for them, including their own preferences. Some proponents of using algorithms in health care delivery claim that more complex algorithms can successfully predict the best treatment plan for an individual based on a range of factors. However, the degree to which an algorithm works depends on how closely a patient matches the population reflected in the underlying data and on how well the algorithm accounts for all the relevant factors in their life, whether the factors are objective empirical issues or subjective values and preferences. Many algorithms do not even claim to account for patient preference, giving patients only the option to be considered compliant or not. As discussed in the next section and in Section IIA, the data underpinning these algorithms is influenced by structural racism in health care research, access, and quality, so reliance on population-level data is less likely to lead to quality care for individuals who are racial and ethnic minorities.

---


The problem of applying population-level data is exacerbated when a hospital or health system uses an average as a benchmark for clinical performance. Clinical algorithms provide recommendations for treatment decisions, such as how long a patient should stay in the intensive care unit (ICU). When doctors know their performance is measured by the average number of hours their patients stay in the ICU, they may feel pressured to send on any patient who stays longer than that average. That pressure is the point of instituting clinical algorithm benchmarks, which are sold promising increased efficiency and reduced costs. However, that pressure will disadvantage the patients who need the longer stay. Moreover, if a doctor’s patient load skews less healthy than the data mix underlying the algorithm, the doctor will have to choose between risking their patients’ lives by moving them out of the ICU early or damaging their career by missing the benchmark. Forcing doctors to make that choice may lead to racial bias because disparities in health care access mean Black, Indigenous, and other people of color are more likely to have underlying conditions that complicate treatment. In addition, residential segregation means that racial groups are likely to be concentrated in certain health care facilities. Therefore, unless explicitly analyzed and validated, Black, Indigenous, and other people of color are more likely to be treated by a doctor whose patient load skews less healthy than the benchmark population. Moreover, even if explicitly analyzed and validated, an algorithm’s recommendation may be inappropriate for a particular patient regardless of their race or ethnicity.

The mismatch between population-level data embodied in clinical algorithms and individual patients has an impact on quality of care, and is one mechanism by which use of algorithms contribute to poor care for Black, Indigenous, and other people of color, RFI question 6. NNU urges AHRQ to investigate the inherent limitations of algorithms to determine appropriate individual patient care and the disparate impact on racial and ethnic lines of those limitations.

B. The medical evidence base underlying clinical algorithms reflect racial bias in health care research, access, and quality.

Clinical algorithms based on available medical research are often designed without regard to relevant differences among patients. Thus, they often perform poorly for particular subgroups of patients. The influence of structural racism on access to health care, quality of health care, and inclusion in clinical studies means that Black, Indigenous, and other people of color are often

---


poorly represented in the medical evidence base. Therefore, recommendations made by clinical algorithms are less likely to be the best choices for their care—whether or not the algorithms explicitly incorporate race or ethnicity as input factors.

Race and ethnicity influence how closely a patient resembles the population underlying algorithmic decisions. They are also correlated with conditions that make some treatment more or less effective, particularly those related to poverty. As Robert Hamm and Zsolt Nagykaldi summarize in the *Journal of Cognitive Engineering and Decision Making*:

A larger issue is that there are specific patients who are not well served by guidelines. As Klein, Woods, Klein, and Perry (2016) and Falzer (2018) argue, although an [evidence-based clinical practice guideline (EB-CPG)] will, by design, produce better results for typical patients, those commonly included in the supporting studies, a guideline’s recommendation may be inappropriate, infeasible, or harmful for other patients. Exceptions may be needed based on patient medical situation (comorbidities, age), patient preferences and goals (Mold, 2017; Mold, Hamm, & Scheid, 2003), patient competence (inability to adhere to, or understand and stick to, a treatment plan), patient social situation (addiction, homelessness, unreliability about clinic appointments), or patient economic situation (inability to pay for visits, prescriptions, or a healthy diet). With EB-CPG regimens, situations can arise where physicians are penalized for doing what they know will be best for a patient. Unless there is allowance for exceptions, a reward regimen can punish those physicians who use more effort and judgment to make better choices for their patients. This can exacerbate physician income differences contingent on the wealth of the patients served: When the measured conformance to a guideline depends partly on patient behavior, the regimen rewards those physicians who are already better rewarded because they serve patients with orderly middle or upper-class lives and a higher capacity to become or stay healthy.7

The Institute of Medicine (IOM) made a similar observation—that clinical practice guidelines are often inappropriate for certain populations—when it issued best practices for guideline development in 2011. After a thorough review of the processes used to develop clinical practice guidelines, IOM concluded that “evidence supporting clinical decision making and [clinical practice guideline] development relevant to subpopulations, such as patients with comorbidities, the socially and economically disadvantaged, and those with rare conditions, is usually absent.”8 Structural racism in the U.S. means that Black, Indigenous, and other people of color are more likely to be poor and have less access to health care throughout their lives than

white people. As we are seeing in the COVID-19 pandemic, this means these groups are more likely to have comorbidities that limit their participation in clinical trials or an economic situation that can affect their ability to maintain the kind of consistent treatment plan assessed in clinical trials. Research into clinical trial diversity bears this out.

Clinical trials often fail to include enough people of color to ensure that their results reflect patient diversity. In the Food and Drug Administration (FDA) snapshot of participants in global drug trials between 2015 and 2019, 76% of participants were white, 11% were Asian, 7% were Black/African American, 5% were marked as “other”, and 1% were American Indian or Alaskan Native. The percentage of white people in the U.S. population is similar, 76.3%. However, the percentage of Black people in the U.S. population, 13.4%, is substantially higher than the 7% in trials. Only 13% of global clinical drug trial participants were Hispanic or Latino, compared with 18.5% of the U.S. population. Thus, algorithmic recommendations based on evidence from these trials will represent white patients better than Black patients and non-Hispanic or -Latino patients better than Hispanic or Latino patients, both in absolute terms and relative to their representation in the U.S. population.

Algorithm developers sometimes attempt to account for these disparities by encoding race or ethnicity into their algorithms. However, including race and ethnicity explicitly in a clinical algorithm can also end up perpetuating disparate health care access. Health outcome differences that appear to be attributed to race, which is a social construct and not a biological reality, may be more correctly tied to correlated factors that the algorithm does not measure, such as socioeconomic status or muscle mass. In these cases, the use of race as a proxy for these factors will make the algorithm a poor fit for individuals of the targeted race who do not share the same correlated factor as the original data set. Racism’s effects are pervasive but vary by context. Correlations with race and other factors may be very different between a study population and the ultimate patient population and will certainly not apply to every individual. The broad application

---


of a clinical algorithm without the treating health care provider’s ability to deviate based on their professional judgment and on the needs and preferences of individual patients can introduce errors into the care of these patients.

The racial bias in the data underlying clinical algorithms has an impact on quality of care, clinical outcomes, quality of life, and health disparities, RFI question 1, and is one mechanism by which use of algorithms contribute to poor care for Black, Indigenous, and other people of color, RFI question 6. NNU urges AHRQ to investigate the ways that Black, Indigenous, and other people of color are systemically excluded or underrepresented in the medical evidence base that underlies clinical algorithms and how this underrepresentation leads to less accurate recommendations for these patients.

C. **Clinical algorithms reflect the judgment and biases of their creators.**

While clinical algorithms may purport to be an objective analysis of the scientific evidence, in fact their development involves significant use of judgment by their creators and creates the opportunity for creator bias—from conflicts of interest, limited perspective on the lives of racial minorities, or implicit racial bias—to be introduced into the algorithm. To create clinical practice guidelines, panels of experts convene to develop guidelines for a particular medical condition or care situation.\(^\text{14}\) Panels go through a process, which varies from institution to institution, designed, in theory, to determine the best care practices based on the best available evidence. The panel must perform a meta-analysis of a body of evidence that entails establishing the criteria for including a research study followed by synthesizing studies that may be based on conflicting assumptions, disparate patient populations, and heterogenous results.

IOM’s best practices for guideline development called out a lack of “sufficient attention” to “the role of judgment in the derivation of recommendations,” among other issues.\(^\text{15}\) It also listed factors that “commonly undermine the quality and trustworthiness of [clinical practice guidelines]” including:

- variable quality of individual scientific studies; limitations in systematic reviews (SRs) upon which [clinical practice guidelines] are based; lack of transparency of development groups’ methodologies (particularly with respect to evidence quality and strength of recommendation appraisals); failure to convene multi-stakeholder, multi-disciplinary guideline development groups, and corresponding non-reconciliation of conflicting guidelines; unmanaged conflicts of interest (COI); and overall failure to use rigorous methodologies in [clinical practice guidelines] development.\(^\text{16}\)


\(^\text{15}\) Committee on Standards for Developing Trustworthy Clinical Practice Guidelines, Institute of Medicine. 2011, fn 8, at p. 3.

\(^\text{16}\) *Ibid.*
Organizations who develop these guidelines ask their developers to use their judgment to balance different factors, including some that do not directly relate to ensuring the best patient care. For example, Kaiser Permanente uses a guidelines-development approach that includes “formulating recommendations based on quality of evidence, balance of benefits and harms, patient values and preferences, and resource and cost implications.” Thus, costs are considered alongside patient outcomes, and “patient values and preferences” are incorporated on a population, rather than an individual, level. The American College of Physicians uses a similar methodology.

Another crucial issue is that there is not always a clear best choice in prevention, diagnostic, and treatment measures. The “scientific evidence about what to recommend is often lacking, misleading, or misinterpreted.” Experts may disagree about whether a particular practice guideline is the best approach to a health issue. For example, doctors have voiced concerns about a sepsis protocol mandated by the state of New York because it included a step that “may not be beneficial.” In another example from 2014, clinical experts disagreed about whether major new cholesterol and blood pressure practice guidelines were appropriate. A group of 5 dissenters out of the 17 authors of the high blood pressure guidelines published an article against the new guidelines. In discussing these disagreements on high blood pressure guidelines, a Journal of the American Medical Association editorial stated that “guidelines should inform but not dictate, guide but not enforce, and support but not restrict.” Practice guidelines often must “harmonize” across differences in research studies. These judgment calls should be made at the bedside not in a corporate board room.

Finally, practice guidelines may not be trustworthy. The JAMA editorial cited above also stated:

Another risk is that the regulatory process may be used to advance commercial interests that may not be in the public interest. Clinical practice guidelines often make recommendations involving proprietary medical devices and pharmaceuticals. Device and pharmaceutical companies could lobby state governments to include these products in future regulations.

17 Davino-Ramaya 2012, fn 14, p. 60.
22 Krumholz 2014, fn 3.
This risk has been born out in practice. In the early 1990s, the Cochrane Collaboration put out guidelines making high-dose steroids the standard of care for acute spinal cord injury. The sole reviewer of the guidelines was a consultant to steroid manufacturers. Despite skepticism from neurosurgeons in polls, the guidance was widely followed until it was reversed in March 2013 by new Congress of Neurological Surgeons guidelines that found no good evidence for use of the steroids and substantial evidence of harmful side effects including death. This is not an exceptional case. One survey found 71% of clinical policy committee chairs and 90.5% of co-chairs had financial conflicts. While financial conflicts create a different kind of bias than racial or ethnic discrimination, these examples show that judgment calls made by authors of guidelines can twist patient outcomes in serious ways.

The problem of unreliable guidelines is magnified when treatment and diagnosis guidelines make different recommendations based on race and ethnicity. Claims about racial and ethnic differences in medical needs are often based on poor quality evidence. Evidence shows that developers of clinical practice guidelines do not give racial differences the necessary level of scrutiny. One review of the use of race correction in clinical algorithms found that when algorithm developers offer rationales for why race correction is included, their origins can be traced “to outdated, suspect racial science or to biased data.” Other developers offer no explanation for why racial or ethnic differences may exist. When designing the algorithm, they choose to translate correlations between race and outcome into different clinical treatment without understanding why those correlations exist or what they really represent. As shown above, both available data and expert judgment can be affected by the structural racism in society and the health care system.

It is essential that the use of race or ethnicity in clinical algorithms is scrutinized, including whether race or ethnicity are serving as proxies for other factors that should be identified explicitly. Studies must also look at racial differences in recommendations made by algorithms that do not explicitly incorporate race, and in their ultimate patient outcomes. However, it will not be possible to eliminate the use of judgment or the need for individual assessment in care decisions. These judgments should be made at the bedside between the patient and their health care provider, not by a committee based on population-level data. Moreover, the underlying research and the process for developing an algorithm must be available to the health care professionals providing patient care.

Encoding biases into algorithms and taking health care decisions away from patients and providers has an impact on quality of care, clinical outcomes, quality of life, and health disparities, RFI question 1, and is one mechanism by which use of algorithms contribute to poor care for Black, Indigenous, and other people of color, RFI question 6. NNU urges AHRQ to investigate

24 See Lenzer 2013, fn 23.
25 Ibid.
27 Ibid.
the role judgment and bias plays in the development of these algorithms, how to minimize the
effects of that bias, and how to ensure that final judgment calls are made at the bedside by fully
informed clinicians and patients.

II. Algorithms developed through machine learning

Answering RFI question 1 on the estimated impact of these algorithms on quality of care, RFI
question 6 on the mechanisms by which use of algorithms contribute to poor care for Black,
Indigenous, and other people of color, and RFI question 7 on clinician and patient awareness of
bias.

While many clinical algorithms reflect decisions made by human experts, such as clinical
practice guidelines, an increasing number of clinical algorithms are driven by machine learning.
These algorithms pose several risks. Clinical algorithms developed through machine learning can
make serious errors, amplify patterns of bias in the underlying data, and endanger population
subgroups. They are also often opaque to users. This can be because they are “black boxes,” where
even their creators do not know how they work, because of protections for proprietary trade secrets,
or because they require high level technical knowledge to understand. This opacity undermines
patient and professional trust and magnifies the risk to patients from errors. Thus, it is essential
that these algorithms are made transparent and intelligible to their users and to ensure that health
care professionals can override them as needed to provide their patients therapeutic and effective
care that is consistent with their needs and preferences.

A. Machine learning algorithms may be trained on datasets that do not apply to
racial and ethnic subpopulations, leading to bias.

Machine learning algorithms, often referred to as artificial intelligence (AI), are
programmed to find patterns in large quantities of data. They are trained on one set of data and
then used to classify new information based on patterns they detected in the training data. They
are frequently used to make diagnoses or to make predictions based on information in electronic
health records and assign risk levels. Problematically, data from electronic health records often
reflect differential access to health care, quality of care, and other forms of structural racism and
biases. Similarly, Black, Indigenous, and other people of color face discriminatory assessment and
treatment by health care providers because of implicit bias or false beliefs about race which are
entered into their electronic health record and used to train clinical algorithms.

For example, in one recent study, researchers found that models trained on electronic health
record data to predict suicide attempts among patients who had outpatient mental health visits
performed substantially worse for Black patients, American Indian/Alaskan Native patients, and
patients without ethnicity recorded than it did for white, Asian, or Hispanic patients.28 There were

28 Coley RY, Johnson E, Simon GE, Cruz M, Shortreed SM. Racial/Ethnic Disparities in the Performance of
Prediction Models for Death by Suicide After Mental Health Visits. JAMA Psychiatry. Published online April 28,
several reasons for this failure. One was a more limited pool of data on Black and American Indian/Alaskan Native patients and patients without ethnicity recorded. The authors speculated that systemic barriers to affordable, culturally competent mental health care led to lower utilization and therefore sparser records on racial or ethnic minority populations. Practitioner bias and institutionalized discrimination throughout the treatment process means that Black, Indigenous, and other people of color are less likely to be screened or receive high-quality treatment for depression and more likely to experience discrimination in health care settings. The researchers also pointed to evidence that discrimination and low quality care deters health care use: studies showing Black and Asian people were less likely than whites to initiate and continue mental health treatment, and that non-Hispanic Black respondents who had experienced discrimination in health care settings were less likely to opt for talk therapy over medication. The authors also suggested that suicide deaths may be misclassified more often among some groups than others. Setting specific thresholds for intervention for each measured race and ethnic group improved performance somewhat for some groups poorly served by the global thresholds but not for others. In any case, setting race and ethnicity-based thresholds to account for poor predictivity meant that Black and American Indian/Alaskan Native patients would be subject to “unnecessary and possibly intrusive interventions” at a higher rate for the same number of interventions in eventual suicides compared to white patients.

Numerous studies have documented implicit bias in health care providers which may then be recorded in electronic health records used to train algorithms. For example, clinicians are less likely to prescribe pain medications to Black patients than white patients. In one study, fewer opioids were prescribed for Black patients with migraines and back pain, which rely on self-reported pain, than similar white patients, but there was no difference for patients with long bone fractures, which are visible on an X-ray. In another study, Black children with appendicitis in emergency departments were less likely than white children to receive any pain medication for moderate pain and less likely to receive opioids for severe pain. These studies demonstrate that Black patients suffer because their doctors do not trust them with opioid prescriptions or believe them when they say they are in pain. This may be due, in part, to the fact that substantial numbers of white medical students and residents falsely believe that Black people feel less pain than white patients.

29 Ibid. at p. E6.
30 Ibid.
33 Ibid. at p. E5.
people. That belief carried over to rating Black patients’ pain as lower and making less accurate treatment recommendations. Similarly, another study found that physicians showed implicit bias favoring white patients over Black patients that could contribute to racial and ethnic disparities in use of thrombolysis for myocardial infarction.

These examples, and there are many others, demonstrate that racially biased behavior by clinicians is a serious problem that should be addressed through changes in training and education as well as through increased staff diversity. It is also a problem in the so-called evidence base of medical data. If an algorithm were to be created to regulate opioid prescriptions and based on health records data, it could easily end up encoding anti-Black bias and hiding it behind a veneer of objective technology.

Finally, algorithms may exhibit racial and ethnic bias whether or not race and ethnicity have been explicitly factored in as inputs. For example, in 2019, researchers Obermeyer et al. found that an algorithm that did not use race as an input still ended up disadvantaging Black patients in its recommendations because it assumed that patients who use less health care are less sick, thereby making health inequities self-reinforcing. Obermeyer et al. analyzed the recommendations made by an algorithm used by large health systems and payers to target patients for “high-risk care management” programs and found that it assigned sicker Black patients the same level of risk as less-sick white patients. This bias reduced the number of Black patients identified for extra care by more than half. This occurred because the algorithm was using health costs as a proxy for health needs. Structural racism has ensured that Black people in the U.S. have lower access to health care, which means they have both higher health needs and lower health costs.

Discrimination at many different stages of the patient experience introduces bias into health records data and therefore into any clinical algorithm that depends on it. Reduced access to health treatment is pervasive among Black, Indigenous, and other people of color. These groups face higher rates of many diseases and premature death, including infant mortality, than white people.

38 NNU recognizes that analysis of electronic health records, whether by human beings or artificial intelligence programs, could expose implicit biases. However, this does not invalidate the need for clinical algorithms to be transparent and intelligible to their users nor the need to ensure that health care professionals have the autonomy to override them if it is in their patients’ interest.
40 Ibid.
41 See citations in footnote 9, above.
42 National Academies of Sciences, Engineering, and Medicine; Health and Medicine Division; Board on Population Health and Public Health Practice; Committee on Community-Based Solutions to Promote Health Equity in the United States; Baciu A, Negussie Y, Geller A, et al., editors. Communities in Action: Pathways to Health
This is due to social, not biological, differences. People of color are more likely to lack health insurance than white people, usually due to affordability. Locations with majority Black and Hispanic populations are more likely to face primary care physician shortages. Additionally, underserved areas Hospitals in Black neighborhoods may have fewer specialists than those in white neighborhoods. These and many other disparities add up to less and lower-quality care, which means less representation in health data. When embedded in electronic health records used to train clinical algorithms, these algorithms reinforce and reproduce both structural racism and implicit clinician bias.

B. Machine learning algorithms may draw inferences from data that are not relevant to health care, potentially introducing racial bias.

One of the most disturbing problems with machine learning is that it may draw spurious inferences based on data that is not relevant to patient care. Moreover, because many algorithms are opaque, as discussed in the next section, it is not always clear what information an algorithm is using to make its categorizations.

For example, a group of Stanford computer science students, in consultation with radiologists, used a set of over 100,000 chest X-rays tagged with diagnoses to teach a program to read similar X-rays for signs of tuberculosis. The algorithm appeared to reach the correct diagnosis 75% of the time. Tuberculosis can be a challenging diagnosis for doctors in South Africa, where it is prevalent, so the project hoped to combine machine and human expertise for a better combined success rate. To make sure it was working correctly, the team designed the program to highlight the parts of the image it was using to make the diagnosis and shared it with others in the field to critique. Fortunately, a medical resident discovered that the X-ray analysis program was basing its diagnosis in part on the information on the edge of the scan image that showed the type of machine used to take the scan. If the machine was of the portable type used in hospitals, instead of the type used in doctors’ offices, the diagnosis was more likely to be tuberculosis. The machine had found a pattern on the images, but it was not in the medically relevant data that it was intended to analyze. In a system where both certain diseases and the ability to access care in certain
venues is highly correlated with poverty and race, this type of unexpected behavior has the potential to introduce bias.

Machine learning algorithms consistently make more obvious errors, leading experts in the field to insist on the importance of a human override option. If an algorithm continues learning from new data while operating, its results can become truly strange. Machine learning algorithms can be easily fooled—Google image software identified a picture of a cat as guacamole after MIT students changed a few pixels.49 To explain the necessity of a human override, one public health expert compared black box algorithms to a plane where autopilot said the plane was going up and pilots saw it was going down but had no override option.50

Inappropriate inferences from data have a negative impact on quality of care, clinical outcomes, quality of life, and health disparities, RFI question 1, and are one mechanism by which use of algorithms contribute to poor care for Black, Indigenous, and other people of color, RFI question 6.

C. Machine learning algorithms can be dangerously opaque making it difficult to identify racial bias in their development or underlying data.

There are several reasons that machine learning algorithms are frequently opaque, but none of them are inevitable. If developers of these algorithms and the health care providers who implement them commit to transparency principles, many systems can be made transparent. If they cannot be made comprehensible to users and patients, they generally should not be used for medical applications.

Some machine learning algorithms function as “black boxes.” Their creators can show that they categorize input data correctly some percentage of the time but cannot explain the reasoning behind the categorizations. The complexity of their reasoning and the number of data points they use to reach conclusions may be difficult for a human to comprehend. They may use a complex form of mathematical representation which is not intelligible for humans.51 An algorithm that is designed to be comprehensible might be less useful, if the goal is to interpret data at a higher level of complexity than a human expert can.52 Moreover, the decision logic may change over time as the program learns.

The black box is an easier design choice to program, but it is often not the only or the best option. Some programmers create black boxes that give hints about their reasoning, such as the X-ray image highlighting that allowed researchers to spot flaws in the tuberculosis diagnosis

50 Ibid.
52 See Ibid. at p. 5.
algorithm. However, these clues do not give a full understanding of what an algorithm is doing and may provide a false sense of security to users. The need for this opacity may be overstated. One computer scientist, Cynthia Rudin, said “I've worked on many predictive modeling problems... and I've never seen a high-stakes decision where you couldn't come up with an equally accurate model with something that's transparent, something that's interpretable.” She explains that medical decisions with life-or-death consequences merit the extra effort to build a program based on clinical knowledge that allows humans to see how it reaches its conclusions.

Creators of algorithms can also avoid transparency to protect their trade secrets. Avoiding sharing information with competitors may be an incentive to design a black-box model or to keep the information about an algorithm restricted inside the corporation that owns it. One observer of financial algorithms argued that corporations also choose to keep algorithms opaque to hide “sidestepped regulations, the manipulation of consumers, and/or patterns of discrimination.” Developers of certain algorithms may also keep them secret to prevent users from changing their behavior to achieve a particular result from an algorithm. For instance, a search engine may keep its inner workings secret to prevent websites from gaming the system.

Sometimes algorithms have information about how they work publicly available, but that information can only be understood by people with a high level of technical knowledge. Most medical professionals, patients, and journalists do not have the appropriate education or the time to read computer code to understand the algorithms governing care.

If a system is opaque, then researchers, users, and patients are limited in their ability to detect and counteract biases. As shown above, there is a serious risk that these algorithms will have biases. Biased data or flawed reasoning can be hidden behind a veneer of objective technology if a machine learning algorithm cannot or does not show its work in a way users and patients can understand. This can have devastating results for individual patients and increase overall health care inequities. Transparency can and should be required, however. It is essential that corporations make their code available to the public, along with appropriate documentation, and that they explain how the algorithm functions so that clinicians can make informed decisions and explain them to their patients. Some types of algorithms will not be appropriate for medical use, despite some promising features, because they cannot be made intelligible to their users. Experiments to check for discriminatory outputs are essential but do not obviate the need for transparency. These measures are essential to safe and trustworthy implementation of this technology.

53 See Ibid. at p. 9; Harris 2019, fn 47.
55 See Harris 2019, fn 47.
56 See Burrell 2016, fn 51, at p. 4, summarizing arguments from Pasquale, Frank. The Black Box Society: The Secret Algorithms that Control Money and Information. 2015.
57 Burrell 2016, fn 51, at p. 4.
58 Ibid.
Users and patients are often unaware of the inclusion of variables that can introduce bias in clinical algorithms, RFI question 7, due to the opacity of machine learning algorithms. NNU urges AHRQ to investigate how machine learning algorithms produce errors and perpetuate bias as well as support both their full transparency and the autonomy of clinicians to fully exercise their professional judgment. NNU supports regulation of clinical algorithms to ensure results are unbiased and reasoning is transparent.

III. Preliminary results from an NNU survey on clinical algorithms suggest that RNs are often prohibited from overriding algorithms, preventing them from correcting mistakes made by biased algorithms.

Answering RFI question 1 on the estimated impact of these algorithms on quality of care and RFI question 6 on the mechanisms by which use of algorithms contribute to poor care for Black, Indigenous, and other people of color.

Clinical algorithms and technology could serve as tools that assist health care professionals in making decisions about patient care, in consultation with the patient and in the patient’s best interests. In practice, however, nurses and other health care professionals are often compelled by their employers, or the health system in which they practice, to accept the recommendations of these clinical algorithms without the autonomy to override them regardless of whether the recommendation is appropriate for and in the best interests of individual patients.

Clinical guidance is designed to be used in concert with direct care professionals’ expertise to find the best treatment for an individual patient. In practice, however, employer rules discourage or prohibit the use of autonomous professional judgment and require adherence to decisions made by clinical algorithms. This limits the ability of health care professionals to counteract biased or inappropriate algorithmic recommendations. Addressing bias in algorithms is necessary but not sufficient to ensure safe, high-quality therapeutic care that meets the needs of an individual patient. Every patient is different, even those who share many demographic and medical history commonalities, and algorithms cannot account for all the relevant differences among patients. To ensure appropriate care is provided, health care professionals must have the right to override algorithms to account for individual needs and preferences.

As discussed above in Section IIA, Obermeyer et al. discovered that an algorithm that was supposed to identify patients in need of extra care failed to identify large numbers of Black patients because it relied on health costs as a proxy for health needs. Optum, the company responsible for the biased algorithm, responded to the research with a statement calling it “misleading” because “[t]he cost model is just one of many data elements intended to be used to select patients for clinical engagement programs, including, most importantly, the doctor's expertise.”

developers of diagnostic algorithms driven by machine learning frequently tout their effectiveness when combined with users’ expertise but stress the importance of an override option. An FDA report on health information technology stated that clinical decision support software “is not intended to replace clinicians’ judgment, but rather to assist clinicians in making timely, informed, higher quality decisions.” Clinical algorithm developers may explicitly state that they are not a substitute for clinicians’ professional judgment and that clinical decisions must consider the characteristics of individual patients, but in practice this is not always the case.

NNU’s members are bedside registered nurses who often face pressure from management and threats of discipline if they deviate from clinical algorithms. Clinical algorithms often are used to reduce the time RNs spend with patients and limit the amount of care they offer them. In mid-April 2021, NNU began surveying RNs and other health care workers, both members and non-members, on their experiences with clinical algorithms in their workplaces, including the use of race and ethnicity as inputs, their awareness of possible bias, and their ability to override recommendations. The survey was initially administered in continuing education classes but is now widely available online. This RFI response will focus on the preliminary results from 170 registered nurses. These preliminary results offer evidence of a negative impact of these algorithms on quality of care, RFI question 1, and of one of the mechanisms by which the use of algorithms contributes to poor care for Black, Indigenous, and other people of color, RFI question 6.

Out of 142 nurses who responded to a question regarding overriding algorithms, 36 respondents (25%) said they were not allowed to “override clinical practice guidelines, clinical pathways, or electronic or computer-based tools that [they] believe are not in the best interest of the patient”, 32 respondents (23%) could only do so with the approval of a doctor or supervisor, and 45 respondents (32%) did not even know if they were allowed to override the recommendations. Only 13 respondents (9%) were allowed to override algorithms based on their own judgment. 16 respondents (11%) said the question was “not applicable.”

The fact that a majority of registered nurses who responded cannot override or do not know if they can override algorithms is concerning because 57 (40%) said they had been “been prompted by a clinical practice guideline, clinical pathway, or electronic or computer-based tool to make choices about patient care, patient care staffing, or other clinical issues that [they] believed were not in the best interest of the patient based on [their] clinical judgment and scope of practice” Out of those nurses, 18 (32%) could not override the algorithms at all, while 8 (14%) said they did not know. Twenty-two (39%) needed approval from a doctor or supervisor to override. Only 9 (16%) of RN respondents could override based on their professional judgment without approval.

62 See Krumholz 2014, fn 3.
The need to combat inappropriate recommendations creates deficiencies in care. Worryingly, one RN responded:

[Her employer] calls them BPA’s (best practice alerts) that pop up in the middle of your charting. Sometimes they are useful reminders, but often it leads to nurses following the BPAs instead of exercising their clinical judgment to individualize each patient's needs. I have been told by an educator “you are not supposed to think or question it. Just do what the computer tells you to.”

Another RN commented:

Healthcare should not be one standard protocol for all but that is what it’s turned into. We are not being asked to use our skills, knowledge, or critical thinking abilities. We are now just asked to follow protocols, policies and procedures. It’s disheartening and disappointing because healthcare is becoming more about financial gains & not actual personalized health for each individual as a whole.

Doctors also feel substantial pressure to comply with treatment guidelines prescribed by clinical algorithms. Polls of doctors show that they frequently will follow guidelines that become the “standard of care” even if they do not agree with the scientific conclusions that underlie them, due to fears that they will be penalized for variations from that standard.63 External payers such as insurance companies and government agencies also reward or penalize individual doctors and medical groups based on compliance with guidelines.64 Payers apply these same rewards and penalties to hospitals and other types of health care facilities. Additionally, the health systems implementing clinical algorithms are often responding to promises by manufacturers that they will be able to reduce staffing costs or to financial incentives to implement electronic health records systems, rather than strong data on patient outcomes.

Many discussions of clinical algorithms mention excessive health care costs as a driving factor.65 Achieving the “efficiency” gains promised by clinical algorithms requires forcing health care professionals to comply with their recommendations, despite possible weaknesses in the tools and the need for individualized patient care. When use of clinical algorithms is heavily incentivized, patients who fail to fit those guidelines and expectations suffer. In 2009, an assessment of a pay-for-performance plan in California found that doctors dropped noncompliant patients and refused to treat people with complicated illnesses to prevent bad outcomes from being added to their statistical records.66

---

63 See Lenzer 2013, fn 23.
64 See Hamm, Nagykaldi 2018, fn 7.
65 See, e.g., Committee on Standards for Developing Trustworthy Clinical Practice Guidelines, Institute of Medicine 2011, fn 8. See also Woolf 1999, fn 19.
The literature cited by AHRQ in the RFI includes numerous examples of systemically biased algorithms. It is likely that these studies on racial bias in algorithms represent only a small sampling of the biased algorithms in use, due to obstacles to research on proprietary algorithms. As discussed above, bias is also introduced by the ways in which population-level data can be a poor fit for individual patients. When algorithms make biased decisions on patient care based on race or ethnicity, registered nurses and other health care professionals have the expertise and connection to patients to find the appropriate course of action. These health care professionals can counteract problems in algorithms if they are given the autonomy to do so.

For these reasons, clinical algorithms must serve as guidelines, not rigid protocols. There may be good reasons to deviate from a recommendation in a manner that has been neither authorized nor anticipated. Health care professionals must be free to exercise their professional judgment regarding the care that is appropriate for each patient based on the patient’s particular clinical indications, circumstances, needs, and preferences.

It is also worth noting that these algorithms have been introduced into health care settings to manage and take advantage of the large quantities of data stored about patients through electronic health records systems and diagnostic imaging computers. As we have seen, this means their performance is limited by the quality of data available. This data is often entered by staff, under pressure from their employers as well as time constraints, tasked with recording a tremendous amount of information for billing and insurance purposes as well as inputs for many different algorithms. That means there will always be some mistakes in data pulled from electronic health records. It also means that the more algorithms health care facilities choose to implement, the more time a health care provider must spend facing a computer instead of their patient. This may be particularly problematic for patients who have limited time with their health care providers at under-resourced facilities and who have difficulty trusting health care providers due to previous experiences with racism.

NNU supports laws and regulations, such as AB 858, a bill introduced in California’s state legislature in its 2021-2022 legislative session, that promote patient safety and reduce the risk from biased algorithms by allowing health care professional who provide patient care to exercise independent professional judgment to override health information technology, requiring employers to train workers on the use and limitations of new technology, and requiring consultation with workers before adopting new technology.

As AHRQ conducts its inquiry into bias in clinical algorithms, NNU urges the examination of the ability of health care professionals to use their independent professional judgment to override these algorithms and the role override can play in combatting bias.

IV. Lack of transparency in algorithms and lack of user education on bias impedes use of professional judgment and makes it difficult for health care professionals to detect bias.
Answering RFI questions 7 and 11 on user awareness and education.

In the experience of survey respondents, RNs are rarely aware of the inclusion of race, ethnicity or other variables that could introduce bias in these algorithms and the implications for clinical decision making. Patients are not aware of how these algorithms may bias their care and providers do not communicate this information to patients. This experience is corroborated by extensive evidence on the ways that proprietary algorithms lack the transparency necessary to allow users to evaluate their recommendations.

Opacity in proprietary systems means that health care professionals often do not know how the algorithms reach recommendations for patient care.67 As discussed in Section IIC, the results from electronic systems trained using machine learning can be opaque even to their creators without techniques to ensure transparency. Health care professionals enter a wide range of information into electronic health records systems, some of which informs clinical algorithms. They are often asked to enter race or ethnicity or other information that can in some contexts serve as a proxy for race, such as income, location, or health care usage history. They later see treatment recommendations pop up on screen. They will often not know what information they entered caused that recommendation or how the algorithm reached that conclusion.

Registered nurses are often required to use clinical algorithms but receive minimal education about how algorithms are developed or may influence clinical decision-making. This impedes RN’s ability to effectively assess the applicability of algorithmic recommendations in their clinical practice and impedes their ability to recognize where population-based and possibly biased data does not apply to an individual patient.

NNU’s survey of RNs on clinical algorithms asked questions about the extent to which users and patients are aware of the inclusion of variables that can introduce bias into algorithms, RFI question 7, and the education available on these algorithms, RFI question 11. The preliminary results show that many registered nurses and patients do not know about the risk of bias in algorithms. As of May 10, 74 out of 168 (44%) registered nurses responding responded that they were not aware that clinical algorithms that include race or ethnicity as a factor may introduce bias into patient care. Fifty-five nurses (33%) responded that they were aware and 39 (23%) said they were somewhat aware.

Even among registered nurses who did know about the potential for bias, this awareness did not come from education and training provided by their employers. When asked “Has your workplace provided any education about how clinical algorithms could introduce bias into patient care?”, an overwhelming majority of 153 out of 168 registered nurses (91%) responded “No, I have not received any education about this.” Only three nurses surveyed said “Yes, I have received extensive education about this.”

67 See Ledford 2019, fn 59.
Nurses are not the only ones who are not being informed about the risks of bias in algorithms. When asked if, in their experience, patients were “informed about the use of race, ethnicity, or other factors that could result in bias in algorithms that influence their care,” the majority of registered nurses, 98 out of 167 respondents (59%) said “no.” Five nurses replied “rarely,” five replied “sometimes” while only one nurse responded “always.” 58 nurses (35%) did not know.

When health care providers cannot see explanations for individual decisions recommended by a clinical algorithm, dangerous errors based on bias can persist without being spotted, preventing users from advocating for the fair treatment of their patients. This opacity impedes the ability of registered nurses and other health care professionals to effectively and appropriately incorporate the scientific information represented in the algorithms into their own clinical decisions based on their individual patients. Our members live in the communities they serve and see patients every day. They have important information about how their individual patient or community may differ from wider data trends. They cannot use that information to counteract biases in the data if they do not know what data is included or how it is used.

This is not just a provider and patient education problem. Often, even researchers do not have access to data on proprietary algorithms. Protections for proprietary tools combined with the sensitivity of health care data make comprehensive studies of racial and ethnic bias in recommendations and patient outcomes rare.68 This means that there is limited evidence available for health care professionals who do know about the possibility of bias to review the performance of the particular algorithms they use in their practice.

In our current market-driven health care system, there is often financial pressure to implement such systems at facilities that serve low-income patients who may be both sicker and less able to pay medical bills. Thus, lower-income communities, that are disproportionately communities of color, and their health care providers may be subject to opaque performance systems to determine what resources they receive. This is also a form of bias in algorithmic implementation.

NNU supports measures to increase the transparency of clinical algorithms and to make information on how these algorithms work accessible to health care providers. Before an algorithm is implemented, rules, content sources, and other relevant information should be readily available to health care professionals and posted on a public website. Crucially, health care professionals, patients, and the public should be educated on the inapplicability of population statistics to individuals and clinicians should have, and be made aware of, the right to override technology in the interests of their patients based on their professional judgment.

AHRQ should include in its analysis the extent to which these algorithms are transparent about their inputs, reasoning, and potential for biased recommendations, and the training and

---

68 Ledford 2019, fn 59.
education provided to the health care professionals who use these tools and the patients whose care is affected by them.

V. Conclusion

As AHRQ conducts its inquiry into how clinical algorithms can introduce racial and ethnic bias into health care delivery, there are several essential points to consider that apply to all algorithms, not just those that have already been proven to be biased. First, there are fundamental limits on the ability of algorithms to meet the needs of individual patients, especially when those patients are part of racial or ethnic groups that are less well represented in the data. Second, AHRQ must consider the importance of ensuring that health care professionals have full autonomy to override algorithmic recommendations, within their scope of practice and consistent with their patients’ needs and preferences. Third, transparency and education about all aspects of the creation, use, and impact of these algorithms is necessary to detect and combat bias. Fourth, transparency must extend to clinicians, patients, and the public, including thresholds for recommendations to provide and deny preventive, diagnostic, or treatment measures by race, ethnicity, gender, and other relevant data. Finally, NNU urges AHRQ to support robust regulation of clinical algorithms as medical devices and to ensure that the supporting evidence and reasoning on which clinical recommendations are based are sufficient, sound, transparent, and intelligible and that recommendation thresholds for providing or denying preventive, diagnostic, or treatment measures are transparent to clinicians, patients, and the public.


Sincerely,

Carmen Comsti
Lead Regulatory Policy Specialist
National Nurses United
MEDICARE’S HOSPITAL AT HOME PROGRAM IS DANGEROUS FOR PATIENTS

Introduction ........................................................................................................... 2

I. The Acute Hospital Care at Home Program Cannot Provide Acute Hospital-Level Care in a Patient’s Home................................................................. 3

II. The Acute Hospital Care at Home Program Allows Hospitals to Shift Care to Inappropriate Settings Rather Than Increasing Acute Inpatient Capacity by Investing in Staffing and Infrastructure.............. 7

III. The Acute Hospital Care at Home Program is Vulnerable to Fraudulent Billing Practices......................................................................................... 9

Conclusion............................................................................................................ 10

Notes....................................................................................................................... 11

National Nurses United
INTRODUCTION

Nursing is a highly-skilled profession that is based on scientific knowledge and attention to detail. It demands an ability to address the physical, psychological, and emotional needs of a patient with compassion, empathy, and advocacy to honor the dignity in all people. Registered nurses are essential to providing acute, hospital-level inpatient treatment. Indeed, acute care hospitals that admit Medicare patients are required to provide nursing services at all times: 24-hours a day, seven days a week.

During the pandemic, the Centers for Medicare and Medicaid Services’ (CMS) Acute Hospital Care at Home (AHCaH) program fulfilled a long-sought goal of the hospital industry: full reimbursement at inpatient rates for “treating” patients in their homes. Under the AHCaH program, CMS waives the 24-hour nursing requirement that defines acute inpatient treatment, meaning care is often provided by unpaid family members or left to the patient alone. Moreover, CMS requires only very limited reporting measures from AHCaH participants and has not made any of the data public.1

The hospital industry has been automating nursing and medical decision-making for years, reducing people to a list of symptoms which are then interpreted by technology that is racially and ethnically biased and often excludes relevant details about an individual patient.2 The hospital industry uses this automated approach to justify reducing the number of licensed health care professionals providing patient care and then profits from the reduced labor costs. The hospital industry has used the Covid-19 public health emergency to further exploit the desire to normalize automated care and to shift care to the home.

Finally, the apparent corporate influence on the program is extremely troubling. In November 2020, the Trump administration launched the AHCaH program outside the normal rulemaking process and in record time: CMS senior leadership worked with industry insiders to take “the waiver from concept approval to publication in 8 days[.]”3 CMS acted without a detailed public evaluation of any evidence justifying the program nor any opportunity for the public to review or comment on it, while hospital administrators who wanted the program were closely consulted.4 Indeed, the American Hospital Association (AHA) took credit for CMS’s expansion of the program, stating: “[As urged by the AHA, CMS expanded on its Hospitals Without Walls program by introducing the AHCaH program.”5 Despite the irregular implementation, the AHCaH program grew rapidly. As of July 27, 2022, CMS has approved AHCaH rollouts in 110 health systems, with 245 hospitals in 36 states.6
I. THE ACUTE HOSPITAL CARE AT HOME PROGRAM CANNOT PROVIDE ACUTE HOSPITAL-LEVEL CARE IN A PATIENT’S HOME

CMS’s AHCaH program endangers patients requiring acute hospital-level care by allowing hospitals to treat them in their homes.7 The AHCaH program builds on previous blanket Covid waivers for the hospital industry, including the Hospitals Without Walls program. Blanket waivers allow hospitals to bypass certain CMS requirements so they do not have to apply for an individual waiver, though the AHCaH program does require an individual waiver application. The AHCaH program waives numerous Medicare provider requirements and patient safety standards that apply to acute care hospitals, including nursing, medical, and emergency services requirements.

Specifically, the AHCaH program waives certain CMS Hospital Conditions of Participation, including a key provision which requires “nursing services to be provided on premises 24 hours a day, seven days a week and the immediate availability of a registered nurse for care of any patient.”8 In an emergency, patients in a fully operational hospital can be treated immediately under CMS’s 24-hour nursing services requirement for acute care facilities. But for patients being treated at home, CMS only requires an emergency response to a patient’s home within 30 minutes. From there, a patient may need to be transported to a hospital, a process that can further delay lifesaving care. Moreover, after a doctor performs an initial medical history and physical exam for an AHCaH patient, CMS does not require any additional in-person registered nurse or doctor visits with the patient. Instead, the AHCaH program requires just two in-person patient visits a day by a community paramedic. These lower standards for nursing, medical, and emergency care under the AHCaH program put patients’ lives at risk.

THE ACUTE HOSPITAL CARE AT HOME PROGRAM LACKS THE ONGOING, IN-PERSON ASSESSMENT AND TREATMENT BY HEALTH CARE PROFESSIONALS THAT DEFINE ACUTE-LEVEL CARE

First, the AHCaH program does not and cannot provide patients with the ongoing, in-person assessment and treatment by health care professionals that acute care requires. Although the bulk of patient care in hospitals is provided by registered nurses, hospitals employ a wide variety of health care professionals who are readily available 24 hours a day, including doctors, respiratory therapists, and pharmacists. Within the inpatient hospital setting, RNs and other health care professionals are able to draw on the collective experience of nursing, medical, pharmaceutical, and other staff.9 This knowledge base is lost when a patient’s care is shifted to the home and a patient’s family must provide this care with limited outside support. Some hospitals currently participating in the AHCaH program do not require another person to be present in the home. Instead, they may leave the patient alone for long stretches of time or provide intermittent support from home health aides to supplement the twice daily visits from an RN or community paramedic.10

The AHCaH program is designed to eliminate the in-person, 24-hour observation and ongoing assessment by a registered nurse that is foundational to acute inpatient care. In contrast to inpatient facilities which provide ongoing, in-person assessment by RNs around the clock in a hospital where there is ready availability of other health care professionals, the AHCaH program requires only two in-person visits a day by paramedics or RNs and monitoring that may consist of just two sets of patient vital signs per day.11 Hundreds of studies, spanning decades, have demonstrated the value of higher RN
Staffing levels and reduced patient care loads in improving patient outcomes, including lowering mortality rates and reducing readmissions, infections, falls, and bedsores. Additionally, studies on the skill mix of those providing patient care have demonstrated that substituting lesser-licensed and unlicensed personnel for registered nurses worsens patient outcomes and increases mortality rates, whereas increasing the percentage of personnel providing care who are RNs improves patient outcomes and lowers mortality rates. Finally, intermittent patient visits do not foster the type of inherently holistic care afforded by round-the-clock inpatient acute nursing care. The relational aspect of nursing, the connection between nurse and patient, is integral to patient health and wellbeing and relies on ongoing, in-person interactions. Ongoing RN care ensures the regular assessment of patients’ mental and physical health status. Based on these regular assessments, RNs are able to perform health care examinations and tests without delay.

RNAs are also the last line of defense in preventing medical errors. For example, prior to medication administration, nurses check to make sure that medication is administered with the right dose, right route, right drug, right time, and right patient. Medication errors are more common in patients treated at home than in patients treated in a health care facility. Even when medications are administered correctly, life-threatening reactions can occur. For example, according to a large retrospective study, “[h]ome infusions were associated with 25% increased odds of emergency department or hospital admission on the same or next day after the infusion.” Moreover, the patients receiving home infusions were younger and had fewer comorbidities than those receiving infusions at a health care facility; thus, the increase in emergency department visits and hospital admissions after home infusions may be higher than the study showed. Another recent study, which reviewed 50 patient charts in an AHCAH program, found 14 adverse drug events among 11 patients and 44 potential adverse drug events among 30 patients. Among the 44 potential adverse drug events, the most common issue was patient or caregiver difficulty in administering medications (32%), followed by “unintentional nonadherence (20%), ... potentially inappropriate prescriptions (18%), and lack of medication availability (16%).” Immediate access to emergency care can be crucial to saving the life of a patient experiencing an adverse drug event.

Family members and home health aides are an inadequate and inappropriate substitute for the provision of acute care by skilled and licensed health care professionals. Worse yet, a patient may be at home all alone. As noted above, studies demonstrate that, even in a hospital setting, substituting lesser-licensed personnel for registered nurses increases rates of patient complications, readmissions, and mortality. Family members and home health aides do not have the education and clinical experience to provide acute, hospital-level patient care nor to perform the necessary ongoing assessment of patients. Even the simplest RN-patient interactions involve assessment and evaluation of the patient’s overall condition. Subtle changes in a patient’s skin tone, respiratory rate, demeanor, and affect provide critical information to patient health and wellbeing, which can be easily overlooked or misinterpreted by a family member or unlicensed support staff. Clearly, care in the home by a family member or home health aide plus two in-person visits by an RN or paramedic does not meet the same standards and level of care of acute inpatient care in a hospital. The lack of 24/7 RNs and other health care professionals is likely to lead to higher levels of missed care, medication errors, and miscommunication, leaving patients vulnerable to grave consequences. Burdening family members with care that should be provided by registered nurses and other health care professionals allows the hospital industry to increase its profits at the expense of patient safety.
THE ACUTE HOSPITAL CARE AT HOME PROGRAM ALLOWS A 30-MINUTE RESPONSE TIME TO EMERGENCIES, WHICH ENDANGERS PATIENTS’ LIVES

Further placing patients at risk, the AHCaH program does not require the immediate availability of emergency response services by licensed health care professionals.

In the AHCaH program, CMS requires an emergency response within 30 minutes rather than requiring that an emergency response be available immediately.24 Without immediate attention from health care professionals and access to necessary treatment resources, patient morbidity and mortality rates increase.25 In contrast to the AHCaH program, most acute care hospitals have trained and certified staff readily available to respond to emergencies. These emergency response teams most often consist of an RN and a respiratory therapist, as well as either a physician, an advanced practice registered nurse, or a physician assistant.26 It is the registered nurse, based on the regular monitoring and assessing of patient status, who most often initiates the rapid response emergency code. Unlike the AHCaH program, a hospital’s rapid response team can respond within seconds of the emergency code being activated.

Delaying emergency response by 15 minutes or more is shown to increase the likelihood of intensive care unit admission or death in a variety of conditions.27 For example, early recognition and treatment of patients with sepsis and septic shock reduce mortality rates and morbidity.28 Severe cases of sepsis can lead to long-term cognitive impairment and physical disability.29 A delayed response to adverse medication reactions may also have negative health consequences. In a study comparing adverse events among home- vs. facility-administered biologic infusions, discussed above, authors “hypothesize[d]” that “less intensive monitoring, less physician oversight, and lack of immediate access to urgent medical treatment … can result in delayed care and a more frequent need for escalation of care.”30 Finally, studies demonstrate that delays by emergency response teams lead to increased mortality and morbidity rates in cardiac arrest events, while a rapid response from the team leads to improved patient outcomes.31 Delaying cardiopulmonary resuscitation when a cardiac arrest occurs leads to higher mortality rates and a greater likelihood of brain damage and associated neurological deficits. For every minute without CPR, the likelihood of survival from cardiac arrest decreases by 7 to 10 percent.32 Assuming that AHCaH programs are treating patients actually in need of acute hospital-level care, because the AHCaH program does not require the immediate availability of emergency response teams as is required in acute hospital settings, CMS should expect mortality and morbidity rates to rise among patients cared for under the AHCaH program.
THE ACUTE HOSPITAL CARE AT HOME PROGRAM FAILS TO PROVIDE THE APPROPRIATE LEVEL OF SERVICES, EQUIPMENT, AND INFRASTRUCTURE NECESSARY TO PROVIDE ACUTE HOSPITAL-LEVEL CARE

In addition to the unavailability of health care professionals, patients’ homes lack the full complement of resources available in a hospital setting to respond to unexpected complications or deterioration of patients’ health status. Although the AHCaH program requires participating organizations to provide laboratory, radiology, pharmacy, and respiratory services, these services are not immediately available in a patient’s home, as they would be in a hospital. In many instances, these services and medical supplies are crucial. For example, diagnosing sepsis, discussed above, requires blood cultures and lactate measurement, followed by administration of broad-spectrum antibiotic agents if sepsis is confirmed. All of these processes are difficult to complete rapidly outside of an inpatient hospital setting.33 Similarly, resources may be needed to evaluate patients’ respiratory status by checking blood gas and electrolyte levels. Additionally, epinephrine may be needed for resuscitation and dopamine may be needed to stabilize blood pressure. Finally, if a patient needs to be intubated, necessary supplies and radiological services to confirm tube placement are crucial. Ready access to all of these resources is essential to saving patients’ lives.

AHCaH patients are extremely vulnerable in the event of a power, telephone, or internet outage because internet and phone service are lifelines that connect AHCaH patients to nurses and doctors for ongoing care and to emergency services when needed. In contrast to most homes, hospitals caring for Medicare patients must have emergency power and lighting in many hospital areas and battery lamps and flashlights in all other areas.34 Additionally, even though it is not a Medicare condition of participation, many hospitals maintain an emergency power supply for the entire facility. Finally, hospitals treating Medicare patients must have an emergency gas and water supply, which patients’ homes typically lack.35
II. THE ACUTE HOSPITAL CARE AT HOME PROGRAM ALLOWS HOSPITALS TO SHIFT CARE TO INAPPROPRIATE SETTINGS RATHER THAN INCREASING ACUTE INPATIENT CAPACITY BY INVESTING IN STAFFING AND INFRASTRUCTURE

CMS’s AHCaH temporary waiver program, if extended, would accelerate the troubling, long-term trend of hospitals and insurers pushing patients out of hospitals and into more profitable settings at the expense of patient care. Since CMS launched the AHCaH waiver program allowing hospitals to transfer or admit acute care patients to their homes, the hospital industry has been advocating to make the temporary waiver permanent. The AHCaH program is part of a decades-long industrial trend seeking to maximize industry profits, which has led to the steady reduction in acute inpatient services and hospital beds available across the country.

If the CMS waiver is extended or another change is approved allowing acute patients covered by Medicare to receive care at home, the health care industry would use the opportunity to push even more patients out of the hospital and further reduce acute care capacity in the United States. Indeed, in a recent webinar, Dr. Bruce Leff, a leading proponent of AHCaH programs, quipped that once the hospital at home program matures, many hospitals will be “turned into condos.”36

Over the last two years, the Covid-19 pandemic has shown us that the acute care provided in hospitals is essential to the health of our communities and that we cannot afford to have it further whittled away by the profit-hungry hospital industry. Acute inpatient hospital capacity has declined dramatically over the last few decades, as the data below demonstrates:

» **Loss of acute beds:** Over the last 25 years, a period in which the U.S. population increased by 25 percent, the number of acute care beds available was reduced by about 70,000. The United States now has only 2.8 hospital beds per 1,000 people, far fewer than other developed countries.37 In 1994, the United States had 4.3 hospital beds per 1,000 people.38

» **Hospital closures:** Since 1990, about 1,400 general acute care hospitals have closed nationwide, with a net loss of 890 when accounting for openings.39 We have lost 181 rural hospitals since 2005.40 According to the Kaiser Family Foundation, the United States has 19.1 hospitals per 1,000,000 people, while the “Comparable Country Average” is 32.7.41

» **Emergency department closures:** From 1990 to 2009, the number of hospital emergency departments in urban areas declined by 27 percent.42

During the Covid-19 pandemic, the loss of U.S. inpatient hospital capacity increased the overall death rate. The Covid-19 crisis laid bare the devastating impact of the reduction of our acute care capacity. A study published by the Centers for Disease Control and Prevention (CDC) found that, between July 2020 and July 2021, intensive care unit bed use at 75 percent capacity was associated with an additional 12,000 excess deaths two weeks later.43 As hospitals exceeded 100 percent intensive care unit bed capacity, 80,000 excess deaths would be expected two weeks later.44 Another study published by the CDC found significant associations between the availability of hospital-based resources, including beds and staff, and excess Covid-19 deaths.45

There have been numerous reports over the past two years of hospitals becoming overwhelmed with acute patients, Covid-19 and otherwise, with nowhere to send the patients they cannot treat.46 Simply put, our national capacity for acute care, weakened by decades of industry profiteering, resulted in needless
deaths during the Covid-19 health crisis. For example, Tony Tsantinis died while waiting for treatment after finding that 17 hospitals had no room for him. Another man, Ray DeMonia, died in September of 2021 after being turned away from 43 hospitals. Sadly, these stories are not uncommon and are a direct result of the elimination of acute care capacity.

Further allowing hospitals to shift acute care to non-acute care settings, such as patient homes, will exacerbate declining acute care capacity. The AHCAH program allows hospitals to retain inpatient hospital reimbursement rates for inadequate and unsafe care in the home, rather than making desperately needed investment in hospital staffing and infrastructure. National Nurses United (NNU) has detailed several recommendations on how to increase hospital staffing capacity without resorting to crisis standards in our November 2021 report, *Protecting Our Front Line: Ending the Shortage of Good Nursing Jobs and the Industry-Created Unsafe Staffing Crisis*.49
III. THE ACUTE HOSPITAL CARE AT HOME PROGRAM IS VULNERABLE TO FRAUDULENT BILLING PRACTICES

The AHCaH program is highly susceptible to fraud and abuse by hospitals through upcoding and other fraudulent billing practices. As discussed above, acute hospital-level care cannot be provided in patient homes because patient homes lack the defining elements of acute hospital-level care, including 24/7 registered nursing care; rapid response capability; and other necessary services, equipment, and infrastructure. Thus, the perfect patient for an AHCaH program is a patient who does not actually need acute hospital-level care. The AHCaH program provides an opportunity for hospitals to diagnose patients at an inappropriately high severity level, send them home, provide only the sub-acute care the patient actually needs, and then charge CMS for acute-level care. Providing care in patients’ homes allows hospitals to expand care beyond the limits on the number of inpatient acute-care beds available, letting hospitals rapidly expand their existing fraudulent billing practices under the AHCaH program.

The Office of the Inspector General (OIG) at the Department of Health and Human Services found a widespread pattern of hospitals diagnosing patients with a higher severity level than is justified by their health condition to receive a greater reimbursement from Medicare. From FY 2014 to FY 2019, the number of stays at the highest Medicare severity level—and highest reimbursement rate—increased by 20 percent while stays at other severity levels decreased. Meanwhile, the average length of stay for patients at the highest severity level decreased while other levels stayed the same. The OIG concluded that it is likely that hospitals systematically bill Medicare for inappropriately high severity levels. Another analysis ruled out demographic changes as the cause of increases in diagnosed severity and confirmed that upcoding was the likely culprit in spending increases.

Fraudulent upcoding is common among hospitals serving Medicare patients. Indeed, many of the health systems and hospitals currently participating in the AHCaH program have been sued for submitting false claims to CMS as well as other irregularities. Even supporters of providing acute hospital care at home caution that “vigilance against overuse and unnecessary care intensity must remain[.]” Based on past behavior, it seems likely that hospitals participating in the AHCaH program will fraudulently bill CMS for treating patients who do not need acute hospital-level care.
CONCLUSION

NNU strongly urges CMS to withdraw the AHCaH waivers immediately and to discontinue the program. The AHCaH program cannot provide acute hospital-level care in a patient’s home because it lacks the ongoing, in-person assessment and treatment by health care professionals that defines acute care in a hospital inpatient setting. It also fails to ensure the rapid response by health care professionals to deteriorating patient status that is necessary to reduce mortality and morbidity rates. Moreover, it allows the hospital industry to capture windfall profits by dramatically scaling back patient care rather than investing in the necessary hospital staffing and infrastructure that would actually increase acute inpatient capacity. The AHCaH program, established by the Trump administration outside the normal rulemaking process, affords the hospital industry a prime opportunity to expand its fraudulent billing practices. In all, it presents a grave threat to patient care and safety and to the future of U.S. national public health and safety.
Medicare's Hospital at Home Program Is Dangerous for Patients

ENDNOTES


10. There are at least two hospitals or health systems participating in the CMS AHCaH program, Brigham and Women's Hospital (MA) and Presbyterian Health Services (NM) that do not require in-home support for admission to their acute hospital care at home programs. Based on publicly available information, the CMS AHCaH program does not require in-home support services. For example, see the inclusion criteria for the acute hospital care at home program run by Mass General Brigham, which includes Brigham and Women's Hospital, as stated at clinicaltrials.gov under registration number NCT03203759: “Can identify a potential caregiver who agrees to stay with patient for first 24 hours of admission. Caregiver must be competent to call care team if a problem is evident to her/him. After 24 hours, this caregiver should be available for as-needed spot checks on the patient. This criterion may be waived for highly competent patients at the patient and clinician's discretion.” (Available at https://clinicaltrials.gov/ct2/show/NCT03203759.) This clinical trial is discussed in these articles:


Note that CMS cites the first study as providing an “[e]xample of published [i]nclusion and [e] xclusion criteria” here: https://qualitynet.cms.gov/acute-hospital-care-at-home/resources#tab2. But the article does not include information regarding whether a
caregiver must be present in the home as specified in the trial at clinicaltrials.gov.

For example, see:
Ibid.
There are at least two hospitals or health systems participating in the CMS AHCaH program, Brigham and Women’s Hospital (MA) and Presbyterian Health Services (NM) that do not require in-home support for admission to their acute hospital care at home programs. Based on publicly available information, the CMS AHCaH program does not require in-home support services. For example, see the inclusion criteria for the acute hospital care at home program run by Mass General Brigham, which includes Brigham and Women’s Hospital, as stated at clinicaltrials.gov under registration number NCT03203759: “Can identify a potential caregiver who agrees to stay with patient for first 24 hours of admission. Caregiver must be competent to call care team if a problem is evident to her/him. After 24 hours, this caregiver should be available for as-needed spot checks on the patient. This criterion may be waived for highly competent patients at the patient and clinician’s discretion.”
Medicare's Hospital at Home Program Is Dangerous for Patients

(Available at https://clinicaltrials.gov/ct2/show/NCT03203759.) This clinical trial is discussed in these articles:


Note that CMS cites the first study as providing an “[e]xample of published [i]nclusion and [e]xclusion criteria” here: https://qualitynet.cms.gov/acute-hospital-care-at-home/resources#tab2. But the article does not include information regarding whether a caregiver must be present in the home as specified in the trial at clinicaltrials.gov.

Presbyterian Health Services provides another example of an acute hospital care at home program that admits patients into without in-home support. See *Hospital at Home Admission Diagnoses and Criteria* available at https://www.hahusersgroup.org/wp-content/uploads/2021/03/Sample-Criteria-Presbyterian-Healthcare-Services.doc.


42 CFR § 482.41.
35 Ibid.

36 Leonard Davis Institute of Health Economics. 2021, November 12. Health Care at Home: A New Frontier: A Virtual Conversation with Bruce Leff, MD, Craig Samitt, MD, Meena Seshamani, MD, PhD, and Reed Tuckson, MD, FACP, moderated by Rachel M. Werner, MD, PhD. https://ldi.upenn.edu/events/health-care-at-home-a-new-frontier/.


39 The information on hospital closures was aggregated by NNU from various sources. There were three main sources: the American Hospital Association Annual Survey Database Reference Guide for years 1990-2021, which contains information on hospital openings and hospital closures; the Department of Health and Human Services Office of Inspector General published a report each year from 1990-2000 of Hospital Closures; and, for Rural Hospital Closures, The Cecil G. Sheps Center for Health Services Research maintains a database of rural hospital closures from 2005 forward.


44 Ibid.


47 Bebinger M. 2022, January 19. 17 Hospitals Had No Room for This COVID Patient. He Later Died Waiting for Dialysis. NPR. https://www.npr.org/sections/health-shots/2022/01/18/1073881763/patients-dying-while-waiting-for-specialized-care-because-hospitals-are-full.


National Nurses United 2021 Survey of Registered Nurses on Experiences with Clinical Algorithms

Overview

From April 21, 2021 to July 7, 2021, NNU surveyed registered nurses (RNs), advanced practice registered nurses, and other health care workers, both members and non-members, on their experiences with clinical algorithms in their workplaces, including the use of race and ethnicity as inputs, their awareness of possible bias, and their ability to override recommendations. This analysis covers the results from 1,042 RNs who responded to one or more of the questions discussed below. The results are based only on those RNs that responded to a particular question.

These results provide evidence of the negative impact these algorithms often have on quality of care generally and of one of the mechanisms by which the use of algorithms contributes to poor care for Black, Indigenous, and other people of color.

Lack of transparency in algorithms and lack of user education on bias impedes RNs use of professional judgment and makes it difficult for health care professionals to detect bias.

Registered nurses are often required to use clinical algorithms but receive minimal education about how algorithms are developed or how they may influence clinical decision-making. This impedes RN’s ability to effectively assess the applicability of algorithmic recommendations in their clinical practice and impedes their ability to recognize where population-based and possibly biased data does not apply to an individual patient.

NNU’s survey of RNs on clinical algorithms asked questions about the extent to which users and patients are aware of the inclusion of variables that can introduce bias into algorithms, and the education available on these algorithms. The results show that many registered nurses and patients do not know about the risk of bias in algorithms. Four hundred nineteen (40.7%) registered nurses responded that they were not aware that clinical algorithms may introduce bias into patient care. Three hundred ninety-one nurses (38.0%) responded that they were aware that clinical algorithms may introduce bias into patient care and 219 (21.3%) responded that they were somewhat aware.

Unfortunately, very few of the registered nurses who responded to the survey received any education and training from their employers. When asked “Has your workplace provided any education about how clinical algorithms could introduce bias into patient care?”, an overwhelming majority registered nurses, 873 out of 1,023 (85.3%), responded: “No, I have not received any education about this.” Only 16 (1.6%) of nurses responded: “Yes, I have received extensive education about this” and 65 (6.4%) responded: “Yes, I have received some education about this.” Sixty-nine (6.7) responded that it was “not applicable.”

Nurses are not the only ones who are not being informed about the risks of bias in algorithms. When asked if, in their experience, patients were “informed about the use of race, ethnicity, or other factors that could result in bias in algorithms that influence their care,” the majority of registered nurses, 551
(54.0%) said “Never.” Forty-nine (4.8%) of RNs responded “Rarely,” 29 (2.8%) replied “Sometimes” and only 17 (1.7%) responded “Always.” Three hundred seventy-five (36.7%) did not know.

**RNs are often prohibited from overriding algorithms, preventing them from correcting mistakes made by biased or inaccurate algorithms.**

NNU’s members are bedside registered nurses who often face pressure from management and threats of discipline if they deviate from clinical algorithms. Clinical algorithms often are used to reduce the time RNs spend with patients and limit the amount of care they offer them.

Out of 795 RNs who responded to the question regarding overriding algorithms, 172 respondents (21.6%) said they were not allowed to “override clinical practice guidelines, clinical pathways, or electronic or computer-based tools that [they] believe are not in the best interest of the patient”, 200 respondents (25.2%) could only do so with the approval of a doctor or supervisor, and 204 respondents (25.7%) did not even know if they were allowed to override the recommendations. Only 117 respondents (14.7%) were allowed to override algorithms based on their own judgment. 102 respondents (12.8%) said the question was “not applicable”.

The fact that a majority of registered nurses who responded cannot override or do not know if they can override algorithms is concerning because 246 (31.0%) said they had been “been prompted by a clinical practice guideline, clinical pathway, or electronic or computer-based tool to make choices about patient care, patient care staffing, or other clinical issues that [they] believed were not in the best interest of the patient based on [their] clinical judgment and scope of practice” Out of these 246 nurses, 76 (30.9%) could not override the algorithms at all, while 41 (16.7%) said they did not know. Eighty-three (33.7%) said they needed approval from a doctor or supervisor to override. Only 42 (17.1%) of RN respondents could override based on their professional judgment without approval. Three responded “not applicable” and one did not respond to this question.

Below are some RN responses to the question: “Is there anything else you would like to tell us about the use of algorithms or about bias in your workplace or clinical practice?”

<table>
<thead>
<tr>
<th>All care these days seem more &quot;cookie cutter&quot; rather than individualized. I was unaware how race influenced these algorithms.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare should not be one standard protocol for all but that is what it’s turned into. We are not being asked to use our skills, knowledge, or critical thinking abilities. We are now just asked to follow protocols, policies and procedures. It’s disheartening and disappointing because healthcare is becoming more about financial gains &amp; not actual personalized health for each individual as a whole.</td>
</tr>
<tr>
<td>[My employer] calls them BPA’s (best practice alerts) that pop up in the middle of your charting. Sometimes they are useful reminders, but often it leads to nurses following the BPAs instead of exercising their clinical judgment to individualize each patient’s needs. I have been told by an educator &quot;you are not supposed to think or question it. Just do what the computer tells you to.&quot;</td>
</tr>
<tr>
<td>Our Assistant managers audit everything and come to talk to you to change your assessment to match employers criteria regardless of assessment.</td>
</tr>
<tr>
<td>The algorithm within [brand name] does not capture the true care of the patient. Which gives patients less care than they deserve.</td>
</tr>
</tbody>
</table>
### Survey Data

<table>
<thead>
<tr>
<th>Are you aware that clinical algorithms may introduce racial, ethnic, and other biases into patient care?</th>
<th>Yes</th>
<th>Somewhat</th>
<th>No</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of RNs</td>
<td>391</td>
<td>219</td>
<td>419</td>
<td>1029</td>
</tr>
<tr>
<td>Percentage of RNs</td>
<td>38.0%</td>
<td>21.3%</td>
<td>40.7%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Has your workplace provided any education about how clinical algorithms could introduce bias into patient care?</th>
<th>Yes, I have received extensive education about this</th>
<th>Yes, I have received some education about this</th>
<th>No, I have not received any education about this</th>
<th>Not applicable</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of RNs</td>
<td>16</td>
<td>65</td>
<td>873</td>
<td>69</td>
<td>1023</td>
</tr>
<tr>
<td>Percentage of RNs</td>
<td>1.6%</td>
<td>6.4%</td>
<td>85.3%</td>
<td>6.7%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>In your experience, are patients informed about the use of race, ethnicity, or other factors that could result in bias in algorithms that influence their care?</th>
<th>Always</th>
<th>Sometime s</th>
<th>Rarely</th>
<th>Never</th>
<th>I don't know</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of RNs</td>
<td>17</td>
<td>29</td>
<td>49</td>
<td>551</td>
<td>375</td>
<td>1021</td>
</tr>
<tr>
<td>Percentage of RNs</td>
<td>1.7%</td>
<td>2.8%</td>
<td>4.8%</td>
<td>54.0%</td>
<td>36.7%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Have you been prompted by a clinical practice guideline, clinical pathway, or electronic or computer-based tool to make choices about patient care, patient care staffing, or other clinical issues that you believed were not in the best interest of the patient based on your clinical judgment and scope of practice?</th>
<th>Yes</th>
<th>No</th>
<th>I don't know</th>
<th>Not applicable</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of RNs</td>
<td>246</td>
<td>416</td>
<td>86</td>
<td>46</td>
<td>794</td>
</tr>
<tr>
<td>Percentage of RNs</td>
<td>31.0%</td>
<td>52.4%</td>
<td>10.8%</td>
<td>5.8%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>
Are you allowed to override clinical practice guidelines, clinical pathways, or electronic or computer-based tools that you believe are not in the best interest of the patient?

<table>
<thead>
<tr>
<th>Yes, without approval from a supervisor or doctor</th>
<th>Yes, with approval from a supervisor or doctor</th>
<th>No</th>
<th>I don't know</th>
<th>Not applicable</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of RNs</td>
<td>117</td>
<td>200</td>
<td>172</td>
<td>204</td>
<td>102</td>
</tr>
<tr>
<td>Percentage of RNs</td>
<td>14.7%</td>
<td>25.2%</td>
<td>21.6%</td>
<td>25.7%</td>
<td>12.8%</td>
</tr>
</tbody>
</table>
Ambient Monitoring

* Other industries have used Ambient Intelligence for years—self-driving cars, retail, logistics—to ambiently understand environments, and provide real-time insights to end users.

* The vast majority of data in healthcare has been manually entered into a system of record—built for generating a bill. Today, healthcare is data-rich, but insights-poor.

* Our goal at [Redacted] is to begin to move to real-time intelligent environments, empowering clinicians with real-time, in-context insights; similar to the way cars now alert their driver when changing lanes or when an obstacle appears.

* We’re starting with baseline use cases first, with a focus on:
  - **Fall Prevention** (identifying when a patient is out of bed, much more accurately and with much less alert fatigue compared to the bed alarm)
  - **Pressure Injury Avoidance** (monitoring for frequency of turning and repositioning and alerting care teams when not performed enough)
  - Potentially growing over time to include use cases like Hand Hygiene Auditing, Rounding Compliance, Incontinence Detection, Medication Disposal, Automated Documentation, etc.

* This all occurs in a secure, private (patient de-identified) manner, leveraging AI—no image data exists, nor is any data ever recorded or stored. Care teams have the power to turn the alerting on or off from a local command center as desired.
technology-enabled process of surveillance, routinization, and interference with professional judgment puts nurses’ health and safety and patients’ lives at risk.

Constant surveillance also means that nurses cannot tell if management is monitoring union activity, such as conversations with union representatives or organizing discussions, which chills union activity and the ability of workers to push back against dangerous management practices. Nurses often are subject to tracking devices that could extend into their private lives and have little knowledge of how employers use their surveillance power. NNU urges OSTP to support robust regulation of AWSM technology in the workplace and by employers generally, to protect the right to collective action as well as employees personal time and privacy.

The federal government must strengthen regulations to limit automated worker surveillance and management technologies to the greatest extent possible. To the extent AWSM technology is implemented, federal regulations should ensure that workers are always notified of the types of surveillance used and the purposes of the data collection. Algorithmic management systems must be entirely transparent, so workers can understand how the decisions governing their working lives are made. Union workers must have the opportunity to bargain over implementation of any AWSM technology before the technology is selected or implemented. Worker control over the implementation and use of AWSM technology in the workplace is the only way to ensure that such systems are implemented without compromising the safety and privacy of workers or their clients. This is particularly true in the health care setting, where privacy and trust are critical to effective patient care, and clinical mistakes due to fatigue or overwork can be fatal.

In the health care context, federal regulations should protect independent exercise of clinical judgment and prevent deskilling of health care professionals. Currently, life and death decisions relating to patient acuity, treatment decisions, and staffing levels are being made by opaque AWSM systems. Recommendations from AWSM systems are meant to inform independent clinical judgment by professionals, but in practice employers often pressure health care professionals to rigidly adhere to AWSM system’s recommendations with the goal of reducing operating expenses. Nurses are expected to follow clinical decisions made by AWSM technology related to patient care and treatment, rather than using their professional judgment in providing care that is consistent with each patient’s unique needs, preferences, and values. Health care professionals often cannot even see the patient data or clinical research that underlies the recommendation and have no way of judging the validity of its application to an individual patient. This puts patients at risk from inappropriate recommendations in the short term and in the long-term results in the deskilling of nurses and creates a dangerous skill gap when atypical or emergency situations arise that the AWSM technology is unequipped to navigate. NNU supports policies that ensure registered nurses and other clinicians can exercise their professional judgment in determining the best course of action for their patients and override decisions made by AWSM technology when doing so is clinically appropriate without threat of discipline or discharge.

Finally, OSTP must strongly warn federal regulators against accepting new models of health care and employment based on the inaccurate and dangerous notion that ambient patient monitoring
technology and algorithmic management can replace in-person care by health care professionals and full employment protections for workers. AWSM technology is enabling dangerous new models of patient care designed to lower labor costs and push patients out of health care facilities, including acute, inpatient-level hospital care at home, telehealth supported by ambient patient monitoring and call center worker tracking systems, staffing platforms that support gig nursing, and other problematic care models that are simply inferior to traditional care at a hospital or other health care facilities, both in terms of nurse employment protections and patient outcomes.

It is essential that OSTP, and the executive branch more generally, supports robust regulation of AWSM technology in health care, particularly technology used in clinical decision-making and staffing, and ensures that recommendations made by such technology serve only as guidelines and are sound, transparent, intelligible, and supported by extrinsic evidence such as in-person examination or observation by a clinician.

NNU’s responses to the RFI questions are below. In some cases, they are repetitive as they are included in each place they were responsive to the question asked.

Sincerely,

Michelle Grisat
National Director of Health and Regulatory Policy
National Nurses United
National Nurses United’s Response to Request for Information: Automated Worker Surveillance and Management

1. **If you are a worker or organization representing workers (such as a worker center, union, or legal services provider), please tell us about your experiences with automated worker surveillance and management systems or the experiences of the workers you interact with, including:**

   a. **The type of work you do (e.g., describe the relevant job, employer, and industry):**

       National Nurses United (NNU) primarily represents registered nurses (RNs). The majority of NNU RNs work in short-term acute care hospitals in both inpatient and outpatient settings but some work in outpatient clinics, medical offices, long-term care facilities, home care, schools, and other settings.

   b. **Whether you are a member of a labor union:**

       National Nurses United, with nearly 225,000 members nationwide, is the largest union and professional association of registered nurses in U.S. history.


   c. **The type of automated surveillance or management you have experienced, including the location of the monitoring technology (such as an app you had to use or download; a device you had to use, carry, or wear; or a camera that monitors you):**

       AWSM systems are distinguishable from traditional surveillance systems in that they draw data from various devices and sources, often operating as part of independent systems, and compile this data into unified data sets, which can then be analyzed to draw conclusions and make decisions that would not be possible from a single system or device. In this sense, AWSM systems are almost always greater and more impactful than the sum of their individual parts. For example, through a combinations of radio-frequency ID tracking in badges, computer-enhanced video-cameras, electronic health records, interoffice communications devices, and even things as innocuous as special sensors on soap dispensers, health care employers are able to produce a 3-dimensional, dynamic representation of the people, objects, and movements within a particular...
environment over time.\textsuperscript{1} This would simply not be possible relying on any one of these technologies alone. Likewise, the vast and disparate nature of the data gathered by these systems\textsuperscript{2} almost always requires that it be processed through a highly complex, and often opaque, algorithm. Most of these algorithms are “black boxes,” where nurses, health care managers, and sometimes even their creators do not know precisely how they work.

Somewhat unique to the health care setting, AWSM systems are also informed and supported by an entire suite of sensors, monitors, and other technology focused on patients and patient care areas. These include sensors that monitor a patients’ vital signs, cameras and other sensors that track a patients’ mobility in their room or throughout the facility, technology to monitor sleep levels, and other types of patient monitoring that can be used to identify and monitor interactions with staff. This patient data is then combined with data drawn from more traditional AWSM systems and synthesized into a comprehensive and dynamic representation of nearly all RN movements and activities, then used to make clinical and employment decisions.

It is therefore inappropriate to think of AWSM systems as discrete technologies, each of which might only have a limited role in the workplace. In reality, these systems generally function together with the shared goal of surveilling and managing employees, lowering labor costs and deskilling nurses by shifting professional care responsibilities to automated, and highly flawed, systems, and attempting to reduce complex RN patient care to computer prompts and box-checking.

In addition to the AWSM systems discussed below, there may be other AWSM systems are actively surveilling and managing our members, but NNU is simply unaware of them. Despite NNU’s consistent and regularly expressed position that employers have a legal obligation to provide notice and an opportunity to bargain over implementation prior to the implementation of an AWSM systems, health care employers often do not disclose the introduction of such systems to NNU and its members. While health care employers, when cornered, often will assert that these are simply updates of older, “dumber” technology, and within their management rights to implement. This is entirely specious. Yet health care employers actually may fear that effective advocacy will derail their plans to deskill RN work and replace them with less costly workers, rather than providing safe and healthy workplaces and fair pay and benefits to attract and retain


\textsuperscript{2} “Ambient sensors will produce petabytes of data from hospitals and homes. This requires new machine-learning methods that are capable of modelling rare events and handling big data to be developed (Table 1)”\textsuperscript{2} Haque, A., Milstein, A. & Fei-Fei, L. Illuminating the dark spaces of healthcare with ambient intelligence. \textit{Nature} 585, 193–202 (2020). \texttt{https://doi.org/10.1038/s41586-020-2669-y}
RN. As a result, some of the AWSM technology and systems discussed in this comment were identified by nurses themselves, while on the job. Given the diverse and low-profile nature of AWSM systems, there is a possibility that there is additional AWSM technology in place that our members have so far failed to recognize.

Researchers studying AWSM technology in hospitals describe a complex and diverse variety of advanced surveillance equipment that could be deployed in health care settings and used to monitor nurse activity throughout their shift. Many if not all of these would be completely invisible to a nurse while performing their duties unless they were informed about the existence of such technology. For example, researchers describe cameras equipped with “inertial sensors,”4 “radio frequency (RF)-based non-contact human movement detectors and geolocators,”5 “passive infrared sensors,”6 “Raspberry Pi Infrared,”7 geolocation enable through Bluetooth technology,8 “temperature-humidity sensor[s],”9 light sensors,10 “thermal imagers,”11 “RGB camera[s],”12

3 The health care industry’s end game is to replace RNs with less costly workers and to create new health care delivery models, including using RNs to lead “patient care teams” rather than provide hands-on care. The health care industry has created the staffing crisis that it is using to justify these changes instead prioritizing patient care and providing safe workplaces that would keep RNs at the bedside. NNU has several recent reports on the industry-created staffing crisis and the failure to provide a safe and health work environment. See Protecting Our Front Line: Ending the Shortage of Good Nursing Jobs and the Industry-created Unsafe Staffing Crisis available at: https://www.nationalnursesunited.org/protecting-our-front-line-report; Workplace Violence and Covid-19 in Health Care: How the Hospital Industry Created an Occupational Syndemic available at: https://www.nationalnursesunited.org/sites/default/files/nnu/documents/1121_WPV_HS_Survey_Report_FINAL.pdf; and Deadly Shame: Redressing the Devaluation of Registered Nurse Labor Through Pandemic Equity available at: https://www.nationalnursesunited.org/campaign/deadly-shame-report.

4 Azevedo-Coste, C.; Pissard-Giblot, R.; Toupet, G.; Fleury, E.; Lucet, J.C.; Birgand, G. Tracking Clinical Staff Behaviors in an Operating Room. Sensors 2019, 19, 2287. https://www.mdpi.com/1424-8220/19/10/2287


“Bluetooth beacons and inertial measurement unit (IMU) sensors,” geolocation using “the range-only extended Kalman filter simultaneous localization and mapping technique,” IMU sensor[s], sound identification through the “percussive source separation technique,” the use of Doppler radar technology, multichannel recording the universal serial bus (USB) microphones, and others technology. Many of the above would be completely invisible when integrated into a health care facility.

In sum, while this comment seeks to respond to the individual questions identified by OSTP in its RFI, it is important to note that each of these systems is generally integrated with the others, and thus their impact on nurses and health care workplaces cannot be analyzed in a vacuum. Each individual system is thus considerably greater, and more insidious, than any one of its individual parts. AWSM systems may therefore be thought of collectively as a single, comprehensive system, of which any one of the technologies discussed below could form a small part.

(1) Electronic health records (EHRs)

The U.S. Office of the National Coordinator for Health Information Technology (ONC) offers this idealized explanation of EHRs:

EHRs are, at their simplest, digital (computerized) versions of patients' paper charts. But EHRs, when fully up and running, are so much more than that.
EHRs are real-time, patient-centered records. They make information available instantly, “whenever and wherever it is needed”. And they bring together in one place everything about a patient's health. EHRs can:

- Contain information about a patient's medical history, diagnoses, medications, immunization dates, allergies, radiology images, and lab and test results
- Offer access to evidence-based tools that providers can use in making decisions about a patient's care
- Automate and streamline providers’ workflow
- Increase organization and accuracy of patient information
- Support key market changes in payer requirements and consumer expectations

One of the key features of an EHR is that it can be created, managed, and consulted by authorized providers and staff across more than one health care organization.

A single EHR can bring together information from current and past doctors, emergency facilities, school and workplace clinics, pharmacies, laboratories, and medical imaging facilities.19

As the description makes clear, the EHR have been integrated into health care operations through policy established by the federal government as well as through financial incentives (discussed below). The EHR interfaces with numerous technologies, including patient vital sign and other monitoring devices; clinical diagnostic, treatment, and prognosis algorithms; clinical datasets; staffing and scheduling software; laboratory and pharmacy ordering systems; billing and payment systems; government quality reporting systems, and health information exchange networks. The EHR, “when fully up and running” is a complex constellation of technologies that creates a digital representation of the patient that serves as a lynchpin to health care restructuring and, with it, the devolution of patient care and worker autonomy. This restructuring includes replacing RNs with patient care teams, remote patient monitoring as well as worker surveillance, management, and automation. The restructuring underway includes the replacement of RNs and other health care professionals with low-cost workers, unpaid family labor, and automation.

In contrast to the rosy picture painted by the ONC, the implementation of EHRs has been plagued by numerous problems with interoperability, errors and bias in embedded clinical diagnostic and treatment recommendations, and faulty patient safety alerts, to name just a few. Indeed, the new Cerner Corporation EHRs used by the Department of Veterans Affairs (VA),

---

have resulted in major harm to veterans, including at least four deaths. The VA recently announced that it would “reset” its implementation of the new multibillion dollar EHR system, halting further implementation while it focuses on problems at five locations using the new EHR. Cerner Corporation was identified as among the top three EHRs in terms of market shares in U.S. hospitals.

(a) The federal EHR incentive program

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, included approximately $30 billion in funding for the EHR Incentive Program. Hospitals and other eligible providers had to demonstrate that they were using their EHRs in conjunction with clinical decision support and computerized provider order entry to receive incentive payments and to avoid penalties that reduced Medicare reimbursement beginning in 2015.

- Clinical decision support (CDS). The U.S. Agency for Healthcare Research and Quality describes computerized CDS as “computerized systems in which software algorithms generate patient-specific recommendations by matching characteristics, such as age, renal function, or allergy history, with rules in a computerized knowledge base.” Although these systems “generate patient-specific recommendations,” they do so based on a fictitious average patient and “match” only a limited set of characteristics. Thus, these recommendations may not be appropriate at the bedside for a particular patient.

To ensure the best care, the “decision support” must serve as a guideline that providers can override if it is not suitable. Yet many hospitals usurp provider judgment by implementing “hard stops” that prevent them from overriding computer “recommendations.” For example, a hard stop may prevent a provider from leaving a computer screen until the provider takes the required action or provides an approved response. Alternatively, the computer may employ a soft stop that, for example, notifies the provider that she is not following the “recommendation” and may include notice that failure to accept the recommendation will be reported to management.

---


Computerized provider order entry (CPOE). CPOE is a type of software program that physicians and other medical practitioners use to enter orders for medication, blood work, imaging, and other types of treatment and testing. It can serve as a replacement for paper order forms, but typically is linked to CDS software that affects the way that orders can be placed. For example, hospitals and medical practice groups may combine CPOE and CDS through the use of computer menu options that limit the types of orders that a medical practitioner can enter.

(b) EHR surveillance and management of RNs

Ostensibly, EHRs are used to track a patient’s progress and document their care. However, in addition to simply recording and tracking patient health information, EHRs differ from traditional medical records in that they then use this information to make recommendations regarding nursing care plans, patient acuity and nurse staffing levels, and nurse performance. Previously all of these determinations were made by nurses and nurse managers through the exercise of their professional judgment.

EHRs accomplish this by processing data entered in the EHR, patient-monitoring data, and data gathered from other AWSM technology, often utilizing proprietary algorithms that are opaque to RNs and other clinicians. EHRs are used to generate a nursing care plan for each patient, assign the patient an acuity level, and determine how many patients to assign to each RN based on the patient’s acuity level and care plan. Staffing levels for the subsequent shift are also determined based on these acuity levels, and nurses are called in for overtime or, for RNs on call for flexible shifts, flexed off as the system dictates.

Significantly, nurses, and often even hospital management, are unaware of what specific information the algorithm is relying on in creating nursing care plans and making acuity determinations. Indeed, some EHR systems hide the acuity score itself from bedside nurses, only making this available to hospital management. This is problematic because it prevents nurses from using their clinical experience and nursing judgment to create a nursing care plan and determine the level of care need. If an algorithm makes an inaccurate acuity determination, a nurse might be unable to provide sufficient care for all the patients for whom they are responsible, resulting in adverse health outcomes for the patient and potential discipline, termination, or loss of licensure for the nurse.

Similarly, nursing care plans are the step-by-step treatment and care plans created by RNs that outline what interventions and procedures a nurse will perform on a patient over the course of their treatment. Prior to the introduction of EHRs, RNs created nursing care plans based on their assessment of the patient and their determination of what would be clinically appropriate based on their education and years of experience. With the introduction of EHRs, nursing care plans are often automatically generated by the system, and RNs are expected to follow what the EHR dictates unless it is clinically inappropriate, in which case they may face significant barriers in changing or overriding the care plan.
Employers are using EHRs to replace RN judgment by automating the creation of nursing care plans and assigning patient acuity levels. RNs develop the nursing skill and judgment necessary to accurately evaluate a patient and create an effective care plan through education and experience in the clinical setting. Determining whether a given nursing care plan will be effective requires experience not only in drafting the plan itself, but in evaluating the factors that determine the type and amount of care that is required. By placing this responsibility in the hands of EHRs, employers’ end game is to introduce problematic new models of patient care that put patients at risk. For example, employers are using “patient care teams” headed by an RN with less costly workers, often unlicensed, replacing work done by previously by RNs.

As health care is not one-size-fits-all. Additionally, tale-tell signs, such as the smell of a patient’s breath, skin tone, affect and demeanor, are often lost on EHR technology, yet are apparent to an experienced nurse and can be crucial to making early diagnostic decisions while there is still time to provide effective treatment. Thus, deskilling nurses also degrades patient care even where the EHR is not making a mistake – such systems simply do not, and cannot, provide the same level of care as an RN. Nurses must be able to alter expected treatment plans based on the unique circumstances of the patient and the patient’s wishes and values and to use their experience and nursing judgment to provide the best course of care. Indeed, they are ethically and legally required to do so. However, they are being pressured by health care management, under threat of discipline or even termination, to conform to decisions made by EHRs that are prone to racial and ethnic bias as well as other errors that arise when one applies information that may apply to a population but not to individual patients.

Finally, and perhaps most obviously, EHRs are used to monitor work processes and identify nurses who management believes are working too slowly or visiting a patient too often relative to the patient’s computer-generated acuity level. These nurses are then pressured, through formal discipline or informal coercion, into working faster and treating more patients with less support, even where they believe doing so will reduce their quality of care. While this helps to optimize hospital profits, nurses who are pressured to work faster are more prone to make mistakes or to fail to identify mistakes made by electronic systems or others. This places patients at risk. The use of EHRs and “black box” decision-making creates several problems for RNs. In many cases, this puts them in the difficult position of being pressured, under threat of discipline, to follow clinical recommendations made by the EHRs without knowing how or why those decisions are made. This is particularly problematic for RNs and other licensed health care professionals who have a professional and ethical responsibility to ensure that their patient is receiving appropriate treatment.

Likewise, this information is then used to second guess nursing judgments that are made throughout the day, such as how much time to spend with a patient, acuity-level and staffing determinations, and even what procedures or interventions should be performed on a given patient at a given time. Nurses that fail to conform to the time or performance expectations dictated by AWSM technology are often “coached,” disciplined, or otherwise coerced into simply following the decisions of the system and working faster, even if they believe that doing so would be unsafe in their professional judgment.
Even more problematic, as a consequence of being pressured to rely on the clinical decisions of EHRs and networked AWSM technology, new nurses will not be able to fully develop the skills necessary to make these decisions independently, while experienced nurses are losing this skill as a consequence of not being able to practice it regularly in the clinical setting. In other words, AWSM technology results in deskillling by shifting crucial clinical decisions, such as determining acuity and the contents of a nursing care plan, to “black box” algorithms, which make these decisions for the nurses, without indicating how or why they are made. Yet, development of these skills is essential for nurses to be able to determine when the AWSM technology has made a mistake and must be overridden, or when the system fails entirely.

(2) Patient monitoring technology

Another form of AWSM technology in the health care setting is biometric and other monitoring devices focused on patients that are used to also monitor and surveille nurse activities. As Suresha, et al. describe: “Recently, non-contact sensors or nearables such as microphones, video cameras, light-intensity sensors, temperature and humidity sensors, are becoming more popular for hassle-free patient monitoring.”25 In addition to capturing patient data, these technologies also pick up “key information about the patient’s ambient environment” including the presence and activity of nurses that are treating them or are in the vicinity. This includes data related to “occupancy and human activity phenotyping,” “medical equipment alarm classification,” and the “geolocation of humans in a built environment.”

Employers claim that patient monitoring technology can reduce nurse workloads, and the need for RN staffing, by substituting for in-person monitoring by nurses. In reality, monitoring sensor output and responding to excessive alerts can increase nurse workloads, interfere with other tasks, and pressure nurses to work faster than is safe to respond to tracked sensor alerts rather than organize their work according to their professional judgment to meet the needs of all patients. Sensor data also serves as input for the next form of AWSM in health care: AWSM ambient intelligence-based patient monitoring systems.

(3) Ambient intelligence-based patient monitoring technology

Health care facilities are beginning to implement comprehensive, ambient intelligence-based monitoring systems that process the information from patient monitoring systems through a computer algorithm, typically in combination with data from other ambient intelligence-based monitoring technology, to produce a 3-dimensional, dynamic representation of the people, objects, and movements within a particular environment over time.26 Peter Y. Chan. et al., define “ambient intelligence” as a system:

---


26 Chan, et al., define “ambient intelligence” to mean a system which utilizes “computer vision-guided neural networks to continuously monitor multiple datapoints in video feeds” using “computer-vision aided infrared
which utilises [SIC] computer vision-guided neural networks to continuously monitor multiple datapoints in video feeds, [and] has become increasingly efficient at automatically tracking various aspects of human movement. For example, it enables automatic tracking of entry and exit into rooms, specific gestures and activities, and interactions between individuals and objects.\(^{27}\)

The ambient intelligence-based monitoring system may then generate output related to patient acuity, staffing, and patient care based on this information, which RNs are pressured or required to follow.

Ambient intelligence-based monitoring systems draw data from traditional surveillance devices, such as video cameras and microphones, specialized sensors (e.g. infrared sensors, radar, and lidar), as well as through digital tracking and metadata from systems that are not principally used for surveillance of health care employees, such as patient’s electronic health records (“EHRs”), cellphones, pagers and other communication devices, and even objects as seemingly innocuous as soap dispensers and identification badges. The vast and disparate nature of the data gathered by such systems\(^{28}\) typically requires that it be processed through a highly complex and opaque algorithm, indeed often times an artificial intelligence or algorithms developed through “deep learning,” which by their nature make it difficult, if not impossible, to determine the clinical basis for the decision. Some of these algorithms are “black boxes,” where even their creators do not know how they work because they were created through machine learning. Other systems are functionally opaque to their users because they require a high level of technical knowledge to understand. In many cases, even the health care employers who opt to implement algorithmic systems may not have access to key information about how the systems work due to protections for proprietary information by the developer.

Somewhat unique to the health care setting, ambient intelligence-based monitoring technologies are also informed and supported by an entire suite of sensors, monitors, and other technology focused on patients and patient care areas. These include sensors that monitor a patients’ vital signs, cameras and other sensors that track a patients’ mobility in their room or throughout the facility, technology to monitor sleep levels, and other types of ambient patient monitoring that can be used to identify and monitor interactions with staff. This patient data is then combined with data drawn from surveilling nurses directly and synthesized into a comprehensive and

---


\(^{28}\) “Ambient sensors will produce petabytes of data from hospitals and homes. This requires new machine-learning methods that are capable of modelling rare events and handling big data to be developed (Table 1)” Haque, A., Milstein, A. & Fei-Fei, L. Illuminating the dark spaces of healthcare with ambient intelligence. *Nature* **585**, 193–202 (2020). [https://doi.org/10.1038/s41586-020-2669-y](https://doi.org/10.1038/s41586-020-2669-y)
dynamic representation of nearly all RN movements and activities, which can then be used to make clinical and employment decisions.

EHRs provide a useful example of how technology primarily used to monitor patients are also used to manage and surveil nurses. As seen in the case of EHRs, such ambient intelligence-based monitoring technology can have a significant effect on the practice of nursing, including how nurses develop essential nursing skills and provide care for their patients. In fact, ambient intelligence-based monitoring and EHRs may be integrated. It is therefore critical that regulations governing ambient intelligence-based monitoring technology also consider and address the degree to which ambient intelligence-based monitoring technology is used to surveil and manage nurses.

(4) Computer-vision aided cameras

One of the most common AWSM technology seen in health care workplaces is computer-vision aided cameras. Computer-vision aided cameras differ from traditional security cameras in important ways. As Chan, et al., describe, computer-vision aided surveillance cameras utilize “computer vision-guided neural networks to continuously monitor multiple datapoints in video feeds” often using “computer-vision aided infrared cameras” and other types of advanced sensors to monitor employee activity. Such systems automatically track various aspects of human movement, including, for example, “automatic tracking of entry and exit into rooms, specific gestures and activities, and interactions between individuals and objects.” Likewise, such systems work together to track nurses, patients and others across wide geographic areas, including between different rooms and work areas, different wards within a hospital, and even between different hospitals.

As with much AWSM technology, the “large volumes of discrete time-series data” gathered by these cameras and imaging sensors are then fed into an algorithm, and combined with data from other AWSM technologies, to create a comprehensive representation of all of a nurse’s actions in a given day, which allows for “observability of granular workplace activity.” The algorithm then, often without any human interaction, makes determinations based on this data regarding patient treatment, RN staffing levels, and nurse performance. Additionally, “cameras and imaging sensors supply data for learning” can be cross-referenced with data from other sources.


30 While it is unclear if the exact ambient intelligence system studied by Chan et al. has been implemented in any US hospitals, our members of confronted a number of highly similar systems in their workplaces.


to further inform how an AWSM system analyzes the data and makes clinical decisions, often without any human intervention or oversight.\textsuperscript{33}

However, the nature of the data being collected, how that data is being analyzed, and what assumptions are being made from that data in clinical decision-making is almost entirely hidden from the clinical professionals who are tasked with overseeing that decision-making process and are ultimately responsible for the health and safety of the patient. NNU has seen first-hand how recommendations made by computer-vision aided cameras and other AWSM technology can interfere with safe, therapeutic health care that meets the needs of each individualized patient. Likewise, such comprehensive tracking interferes with nurses’ right to engage in protected, concerted activity, invades their privacy, is frequently used to support discipline that is entirely unfounded.

\begin{itemize}
\item \textbf{(5) Electronic identification badges}
\end{itemize}

Another common form of AWSM technology in health care workplaces is the use of electronically-enabled identification badges (“ID badge”) to track employees’ movement throughout a facility. In hospitals and other health care facilities, nurses are typically required to swipe their ID badge upon entering the facility, upon entering specific rooms, such as rooms where medication, food, or supplies are located, upon entering certain operational areas, such as radiology rooms or operating rooms, and sometimes upon entering patient rooms. The identity of the nurse, the time of the swipe, and the location of the swipe are all generally recorded, and fed into an algorithm that, when combined with data drawn from other AWSM technology, can create a dynamic representation of their movement and activities throughout the day.

In addition, many ID Badges also now include radio frequency identification (“RFID”), which allows the system to actively track a nurse’s location at all times in a facility as they pass by special RFID enabled sensors, even without swiping, which are distributed throughout the facility. This type of passive tracking allows for even closer surveillance of a employees’ activities, and, significantly, can take place at any time without employees’ knowledge. Moreover, even if it is not actively tracking when a nurse enters a private space, such as a bathroom or their car, as most do, an RFID system can determine when a nurse is in such locations by process of elimination, since it can actively track their movements over time everywhere else in the facility.

The constant tracking of nurse locations through ID badges creates significant privacy concerns, as nurses may be tracked when they are going to the bathroom or engaged in other private activities, or while they are off duty but still at the facility, such as during breaks or before or after their shift. Constant surveillance also chills protected concerted activity, as it allows management to identify who is talking to whom, and from this, determine union leaders and supporters. Even in workplaces that are already unionized, conversations with shop stewards or

union representative may be tracked, and unlawfully used by management in making employment decisions without the nurses or their union ever being aware.

(6) **Cell phones and other communication devices**

Much like ID Badges, nurses have long been expected to carry communication devices to communicate with other staff while on shift. These devices are increasingly being used to passively surveille nurses by feeding data from these devices into AWSM technology. Our members report that hospitals and other health care facilities are increasingly recording and logging all nurse conversations that take place through employer-provided communication devices. In addition to logging the contents of the conversations themselves, these communications can be digitally encoded, and this data can be used to track nurse activity and performance, particularly when combined with data from other AWSM sources.

As with ID Badges, communication devices can be used to determine a nurse’s location at the time a given communication was made, either through using a GPS unit within the device or through triangulating the location through the wifi signal or cell signal used to make the call. Indeed, nearly every smartphone, the primary device used for communication in the workplace by many of our members, is equipped with GPS and a myriad of other technology that allow it to be tracked and located, sometimes even when the device is turned off. Worse still, these devices are sometimes brought home with nurses at the end of their shift, allowing them to potentially be tracked wherever they might bring their cell phone in their free time.

Additionally, communication devices are unique in that, by their nature, they are capable of passively recording ambient sounds. This is particularly true of modern smartphones, which use active listening to allow activation of automated assistants and other accessibility features. This, too, encroaches on nurse privacy and may impede organizing and collective bargaining activities. Indeed, even if these devices are not passively recording employee conversations or tracking employees outside of work hours, the mere potential of such surveillance is enough to effectively chill union activity.

(7) **Hand-washing monitoring**

Hand-washing monitoring systems are another form of AWSM technology used to surveille nurses in health care workplaces. This typically involves camera systems or sensors that monitor hand washing stations. This video and sensor data is then combined with data from other AWSM technology to determine the identity of the nurse, the instances in which they wash their hands, how long they spend washing their hands, how frequently they wash their hands, and other related information, and make determinations and recommendations regarding whether a nurse is complying with hand-washing requirements.

As with all AWSM technology, such systems are problematic to the extent that it is unclear what data is being recorded and how this data is being used. Hand-washing monitoring systems often appear in bathrooms, breakrooms, and other private spaces, where nurses have a reasonable expectation of privacy. It is unclear if such systems are recording or sensing video or audio data,
or how this data might be combined with other data to create a comprehensive depiction of nurses’ activities within these private spaces. Granular surveillance of private activities in bathrooms and break rooms presents clear privacy concerns. It also creates the impression that management is surveilling activity in these locations, which will chill protected concerted activity.

d. Whether the automated surveillance or management was used during a labor organizing drive;

While NNU is not aware of any specific instances in which AWSM technology was used as part of an adverse employment action or to stymie an organizing campaign, the nature of this technology, which allows it to generate a dynamic, real-time account of all nurse activities within a health care facility, means that surveillance of organizing activity inevitably occurs. Employers may be using AWSM technology to take adverse action against nurses for engaging in protected activity based on the information gathered by AWSM technology without explicitly identifying AWSM technology as the basis for the adverse action. The ubiquitous nature of this surveillance inherently creates the impression that nurses are constantly being observed and surveilled by management. Thus, the presence of this technology alone is enough to interfere with nurses’ labor rights and chill protected, concerted activity.

By implementing AWSM technology without limits that prevent surveillance of protected concerted activity and without explaining to nurses, and their collective bargaining representative where relevant, how those systems work, health care employers create the impression of near constant surveillance. Depending on the AWSM technology, this may extend to activities outside of work hours and away from work areas, thereby interfering with protected concerted activity. In addition to providing a more detailed account of a nurse’s daily activities, AWSM technology has the capability of monitoring nurses at times and in locations where they previously were not subject to surveillance, often times through the devices they are required to carry with them, such as cell phones and ID badges. Without relevant information related to how these systems work and an opportunity to bargain over when and how nurses will be monitored, nurses reasonably may assume that they are subject to surveillance at nearly all times. This impression is more or less confirmed when they are shown detailed, three-dimensional images compiled from multiple different data sources depicting their movements and activities throughout the day. (See Attachment 1, examples of imaging technology capabilities provided to National Nurses United by management.) This impression of constant, pervasive surveillance chills union organizing and protected concerted activity. Nurses may fear that they will be identified as union supporters or troublemakers and subject to retaliation if their employer can identify them as a union supporter or a proponent of a collectively bargaining for change in their workplace.
Federal law has long made clear that employees must be free of the interference and coercion caused by employer surveillance during organizing. Likewise, well-established precedent makes clear that even the impression of surveillance can violate the act. For example, in Community Counseling & Mentoring Services, 371 NLRB No. 39, the National Labor Relations Board (NLRB) “held that an employer unlawfully created the impression of surveillance where its president remarked to employees during a staff meeting that he would know if they talked about work issues among themselves because he had ‘eyes’ and/or ‘ears’ at the facility.” Just as in Community Counseling & Mentoring Services, nurses that work as hospitals and other health care facilities that implement AWSM technology know that their employer has “eyes” and “ears” at the facility, and that their employer may know if they talk about work issues among themselves. Thus, as in Community Counseling & Mentoring Services, the mere presence of this type of surveillance technology is sufficient to interfere with nurses’ protected rights and constitute a violation of the Act. Indeed, NLRB General Counsel Jennifer Abruzzo appeared to acknowledge this earlier this year in announcing a partnership with the Consumer Finance Protection Bureau to address practices of employer surveillance, monitoring, data collection, and employer-driven debt, stating “[e]mployers’ practices and use of artificial intelligence tools can chill workers from exercising their labor rights.”

---


35 “The law is equally clear that an employer violates Section 8(a)(1) if it creates the impression among employees that it is engaged in surveillance, because by highlighting its “anxiety” concerning union activities it tends to inhibit an employee’s future union activities.” Higgins, J. E., Arnault, B.T., Bock, R.A., Gaylord, A.M. (2022). The developing labor law: The board, the courts, and the National Labor Relations Act (Eighth Edition.), Chapter 6. Interference With Protected Rights. Bloomberg BNA; (citing, inter alia, Sam’s Club, 342 NLRB 620 (2004) (store manager created impression of surveillance when he told employees he heard the employees were circulating a petition where the petition was not circulated openly); Music Express E. Inc., 340 NLRB 1063 (2004) (employer created impression of surveillance when it told employees where the next union meeting would be held); Golden State Foods Corp., 340 NLRB 382 (2003) (supervisor's comment that “eyes are on you and you need to watch your step” to pro-union employee created impression of surveillance and violated Act).


In order to prevent unlawful interference with employee rights, OSTP must support rules that require health care employers to meet their collective bargaining obligations prior to implementing AWSM technology. This includes providing notice to nurses and their union that the employer intends to implement such systems, proving sufficient information regarding the capabilities and uses of these systems to enable understanding and meaningful bargaining, and bargaining over their implementation and effects prior to implementation. OSTP must also ensure that these systems include limits that prevent them from being used to surveil protected, concerted activity, and that these limits are openly communicated so that employees know when they are and are not being surveilled and recorded.

e. **Whether and when your employer informed you about their use of automated worker surveillance and management systems:**

In addition to the AWSM technology discussed above, it is likely that other types of AWSM technology are actively surveilling and managing our members, but NNU is simply unaware of them. As discussed in NNU’s response to questions 1.c. and elsewhere in these comments, health care employers frequently fail to notify NNU or its members when new AWSM technology is being implemented in the workplace, taking the position that these are simply updates of older, “dumber” technology, and within their management rights to implement without notice to the union or an opportunity to bargain. Thus, some of the AWSM technology and systems discussed in this comment were identified by nurses themselves, while on the job. It is therefore quite likely that other AWSM technology has already been implemented that our members have not yet identified.

The NLRB has long held that it is violation of the National Labor Relations Act to make unilateral changes during the course of a collective bargaining relationship concerning matters that are mandatory subject of bargaining, absent waiver by the union or impasse following good faith negotiations.\(^{38}\) Indeed, this is one of the rare per se categories of prohibited conduct, and is therefore a violation of the NLRA even where the employer is acting under a good faith belief

that it has no duty to bargain.\textsuperscript{39} As Judge Harry Edwards explained in \textit{NLRB v. McClatchy Newspapers}:

A unilateral change not only violates the plain requirement that the parties bargain over “wages, hours, and other terms and conditions,” but also injures the process of collective bargaining itself. “Such unilateral action minimizes the influence of organized bargaining. It interferes with the right of self-organization by emphasizing to the employees that there is no necessity for a collective bargaining agent.”\textsuperscript{40}

It is equally clear that the implementation of ASWM technology constitutes a mandatory subject of bargaining. In \textit{Anheuser-Busch, Inc.}, 342 N.L.R.B. 560, the NLRB held that an employer violated the act by unilaterally implementing surveillance cameras without giving notice or bargaining with the union because the cameras were trained at work and break areas.\textsuperscript{41} In so doing, the Board concluded that “the use of hidden surveillance cameras in the workplace is a mandatory subject of collective bargaining.”\textsuperscript{42} Just as the introduction of mere surveillance cameras constitutes a mandatory subject of bargaining because they \textit{can} record employees in \textit{some} work area, so too does AWSM technology, which creates a comprehensive, dynamic depiction of employees and their actions throughout the day. Thus, by failing to provide notice of the implementation of this technology or an opportunity to bargain, health care employers are clearly engaging in \textit{per se} violations of the NLRA.

Moreover, because of this lack of notice to nurses or their representatives, NNU is likely unaware of the full extent of AWSM technology being used in our members’ workplaces. AWSM technology is myriad and often difficult to recognize. Researchers studying AWSM technology in hospitals describe a complex and diverse variety of advanced surveillance equipment that has been deployed in health care settings and can be used to monitor nurse activity throughout their shift. Many if not all of these would be completely invisible to a nurse while performing their duties unless they were informed about the existence of such technology. For example, researchers describe cameras equipped with “inertial sensors,”\textsuperscript{43} “radio frequency (RF)-based non-contact human movement detectors and geolocators,”\textsuperscript{44} “passive infrared


\textsuperscript{41} \textit{Anheuser-Busch, Inc.}, 342 N.L.R.B. 560, 560 (2004).

\textsuperscript{42} \textit{Anheuser-Busch, Inc.}, 342 N.L.R.B. 560, 563 (2004).

\textsuperscript{43} Azevedo-Coste, C.; Pissard-Gibollet, R.; Toupet, G.; Fleury, É.; Lucet, J.C.; Birgand, G. Tracking Clinical Staff Behaviors in an Operating Room. \textit{Sensors} 2019, 19, 2287. [Google Scholar]

sensors, “Raspberry Pi Infrared,” geolocation enable through Bluetooth technology, “temperature-humidity sensor[s],” light sensors, “thermal imagers,” “RGB camera[s],” “Bluetooth beacons and inertial measurement unit (IMU) sensors,” geolocation using “the range-only extended Kalman filter simultaneous localization and mapping technique,” “IMU sensor[s],” sound identification through the “percussive source separation technique,” the use of Doppler radar technology, multichannel recording the universal serial bus (USB) microphones, and others technology. Nearly all of the above would be completely invisible once integrated into a health care facility.

Finally, and perhaps most significantly, the argument that this is merely an update of older technology that does the same thing is simply spurious. AWSM technology is unique from older forms of surveillance in that it creates an ecosystem of various data sources that are combined through black-box algorithmic processing to produce a dynamic depiction of a nurse’s activities throughout the day that would be impossible from any one sensor or camera. Each individual system is thus considerably greater, and more insidious, than any one of its individual parts. AWSM technologies must therefore be thought of collectively as a single, comprehensive electronic management system, of which any one of the above technologies could form a small part.

**f. Whether you (or, if relevant, your representative, like a labor union) have any input or control over how, where, and over what automated surveillance occurs:**

NNU and the nurses it represents often have little or no input over how, where, and over what surveillance occurs. Health care employers often fail to provide adequate notice or an opportunity to bargain prior to implementing AWSM technology, despite the fact that these system often have a drastic impact on nurses’ terms and conditions of employment. Rather, health care employers typically take the position that such matters fall within their “management rights,” even if there is no clear contract language on this point in the relevant Collective Bargaining Agreement or Memorandum of Understanding. This prevents nurses and their unions from knowing precisely which AWSM technologies are operating in their workplace, how they work, what they are monitoring, and how they are used in clinical and employment decisions until after the are implemented.

Employers generally assert that these powerful AWSM technologies are just updates of older technology that has long been in the workplace, such as treating computer-vision aided cameras the same as traditional security cameras, or EHRs as electronic versions of old paper medical records. However, these technologies are much more than modern iterations of well understood tools. Rather, AWSM technologies pull vast and diverse data from an entire ecosystem of monitoring equipment, such as those described above, and process this information through opaque algorithms that then make clinical and employment decisions.

For instance, around 2017, a large health system located in California did provide notice to NNU that it intended to implement a patient acuity and RN workload program known as Epic Acuity. While it refused to bargain over implementation, claiming that this was within its management rights, it did agree to engage in bargaining over the effects of the new technology. This system replaced the prior system. Like many modern systems, Epic Acuity is a points-based acuity

---

58 This includes things such as staffing levels, privacy, and discipline resulting from time spent on various nursing activities such as rounding, charting, hand-washing, performing various procedures, treatments and interventions, and performing other duties like helping patients bathe or use the restroom.
system that uses an algorithm to review information entered into the EHR by doctors and nurses and based on this information, assigns an acuity score, which was used to determine the number of RNs that would be required in a given department on a given shift.

Almost immediately, this system began to have serious problems. Like other patient acuity and RN workload software, Epic Acuity assumed that RNs and other clinicians had the capacity to update EHRs in real time. Thus, Epic Acuity made acuity and RN workload decisions based on this assumption. However, in reality, overworked RNs are often not able to chart until the last hour of their shift, when the next shift overlaps with theirs and there are extra hands to take on patient-care duties, allowing time to chart. This, however, leads the system to assume that fewer RNs are required on the subsequent shift, which, in turn, leads to RNs on the subsequent shift being overutilized and not having time to chart, causing a vicious cycle.

Likewise, the acuity scores provided by Epic Acuity called for fewer staff than the prior system in the same exact circumstances, leading to fewer RNs available to provide care for sicker, more numerous patients. While Epic Acuity is a “black box” system, and thus RNs are unaware how it makes acuity determinations, NNU was able to secure, through collective bargaining, two worker committees to oversee the transition and implementation of this technology. NNU was also able to secure a one-month transitional period, in which both the old technology and the new technology, Epic Acuity, operated simultaneously. By comparing utilization rates and patient care and direct care hours produced by both systems, these committees were able to determine that in at least two locations, on a daily basis, Epic Acuity was providing fewer RN hours than the previous system for the same patient care unit. Thus, by implementing Epic Acuity, this health system was effectively forcing RNs to care for more patients with less support. While the health system claimed to make changes to the system after NNU reported this problem, NNU was unable to confirm this, as the health system will not provide information regarding what specifically was changed in the algorithm. Likewise, these changes can take months, if not years, to implement, leaving nurses in the lurch while health care management struggles with refining and understanding the technology it has already implemented.

Thus, to the extent the NNU or its members have had any input or control over how, where, and over what automated surveillance occurs, this has been the result of aggressive collective bargaining by the union, and the diligent work of its members in worker committees, comparing output data and drawing statistical conclusions. NNU and its members are not provided the same information as the employer about how this system works or how it will be implemented. Instead, they are typically presented with the introduction of AWSM technologies as a fait accompli and may be given an opportunity to bargain over the effects of its implementation. This is simply insufficient to fulfill the legal obligation of health care employers, or to allow NNU and other unions to protect their members against the abuse of these systems.

In sum, in regulating AWSM technologies, OSTP must ensure that employers provide notice and a meaningful opportunity to bargain over implementation prior to implementation. This technology is simply too powerful and disruptive to be treated as an update of older non-networked technology, nor does this accurately capture the major effect that implementing this
technology can have on nurses’ terms and conditions of employment, as demonstrated above. Anything short of full transparency and bargaining engagement will inherently create the impression among nurses that they are subject to near constant surveillance, and that their words and actions are always being recorded by hidden, advanced monitoring devices, and that this information is being compiled and analyzed by algorithms that then produce a detailed and dynamic representation of everything they do throughout the workday. OSTP must therefore champion regulations that require full and complete transparency prior to the introduction of these technologies, and that ensure health care employers meet and respect their bargain obligations.

g. Whether you know how the data generated by surveillance is used for management or other purposes (including purposes related to employment or labor market competition):

For RNs, questions 1.g., 1.i., and 1.k. are interrelated. NNU’s response to question 1.g. will focus on how health care employers use surveillance data to facilitate workforce restructuring, including deskilling professional nursing and eroding registered nurse scope of practice.

Health care employers use the data generated by surveillance in implementing AWSM technologies and systems, particularly EHRs and other health information technology (HIT), for workforce management as well as to restructure health care delivery, including the workforce. This includes attempts to routinize and deskill the profession of nursing with the goal of replacing licensed registered nurses with lower cost staff, including unlicensed staff, and unpaid laypersons. The health care industry’s aims include replacing RNs at the bedside and instead having them lead patient care teams, sometimes remotely, with lower cost workers doing the work RNs have done previously.

(1) A WS M Systems Lead to the Deskilling of Registered Nurses and Erodes Their Scope of Practice.

Employers are using AWSM technology to deskill professional nursing and erode RN scope of practice. In so doing, they aim to increase their net income by reducing labor costs and capitalizing on the industry-created RN staffing crisis to justify shifting important patient care responsibilities to unlicensed and lesser-licensed staff as well family caregivers and patients themselves. This happens in large part through the routinization of patient care and deskilling of RNs coupled with a shift to telehealth and alternative care settings. Health care employers

frequently mandate as “best practices” those work processes that reduce labor costs and improve their bottom line.

Routinization leads to the deskilling of work processes and health professionals. Skill is the ability, drawn from education and experience, to do something expertly. It can also be defined as the effective exercise of professional judgment in non-routine situations. Following prescribed rules, as a machine would, enables an employee to perform tasks, but it does not make the employee skilled. They can do their job as long as there are no surprises. But when something unexpected happens, the rules break down, yet caring for patients means facing the unexpected every day. Skilled health professionals such as RNs can cope with the unexpected. They know because of their education and experience and are able to rely on their own judgment. The exercise of judgment is the essence of skill.

Health care employers utilize AWSM technologies and algorithmic recommendations regarding staffing, workload, and patient care to routinize work processes, and, to the greatest extent possible, deskill the complex RN profession by reducing it to a series of tasks prompted by a computer screen and entered into the EHR. The health care industry has long worked to fragment complex, holistic RN nursing care into discrete tasks, which can then be routinized with variations eliminated. While this is often touted by employers as a way to raise quality standards, it is typically merely a way to speed up and intensify work. Given that patients are unique and complex, variation of patient care to match the needs, values, and preferences of particular patients is not a defect; to the contrary, it is essential. It is why RNs are valued for their education, experience, and professional judgment.

RNs typically are unable to review recommendations made by AWSM technology. RNs are pressured to work faster and rely on the output of opaque technologies but are also ethically obligated to ensure that the nursing care they provide is appropriate. AWSM technologies, particularly when deployed in health care settings, frequently make determinations and recommendations that are incorrect or potentially harmful. If RNs do not have the information necessary to catch these mistakes, there is no way to prevent these errors from harming patients.

Moreover, RNs typically do not have control over the number of patients assigned to them. In fact, California is the only state that places a numerical limit on the number of patients that can be assigned to an RN providing inpatient hospital care. The limits are based on the type of patient care unit they are working in and can be reduced, but not increased, based on the acuity of the patients assigned. Thus, RNs do not control if they have the time and resources to care for patients. Increasingly, AWSM technology-based acuity systems make staffing determinations.

(2) Algorithmic management systems prevent nurses from exercising and maintaining nursing judgment.

As with RN skill, employers seek to use AWSM technology to minimize the role of RNs’ professional judgment. RNs’ professional judgment reflect their education, expertise, and experience in clinical decision making. Routinizing decision-making processes related to nursing
NNU Comments  
OSTP, Request for Information: Automated Worker Surveillance and Management  
Docket ID: OSTP_FRDOC_0001  
Page 26 of 40

care and reducing those processes to entering data into an EHR in response to computer prompts limits RNs ability to exercise and maintain the efficacy of their professional judgment. To the degree this happens, nurses may lose their ability to recognize and correct errors made by AWSM technology or other providers, problematically making them replaceable with non-RNs, as described above.

Yet the development and use of hands-on nursing skill and judgment when assessing and providing care for a patient is an essential and necessary element for the provision of high-quality nursing care. For instance, sleepiness and dilated pupils can indicate that a patient a suffered a hemorrhagic stroke. Likewise, foul-smelling breath can indicate an abdominal obstruction, whereas breath that smells like Juicy Fruit gum can indicate a patient is suffering from diabetic ketoacidosis. Typically, these observations are made in passing in the course of providing care for a patient, including during activities that are typically not diagnostic in nature, such as helping a patient ambulate or use the restroom. Overreliance on sensors and algorithmic recommendations within facilities and use of models that use ambient intelligence-based patient monitoring to require nurses to provide care remotely, discussed further below, prevent nurses from having the opportunity to make these hands-on observations that are essential for providing quality nursing care.

Moreover, the AWSM systems that facilitate this “remote care” often themselves prevent nurses from using their judgment, even when they are aware that the system is making an error. For instance, one member described an instance in which an AWSM system at the UC Davis Medical Center reported that her patient was septic, even though she knew from 15 years of experience and her own assessment that this was not the case. While the algorithm did not provide the rational for its decision, as is typical with AI-supported AWSM systems, it likely failed to take into account that the patient’s elevated white blood cell count, normally correlated with a septic infection, could have resulted from the fact that the patient also suffered from Leukemia. While the UC Davis Medical Center allows nurses to override the assessment of the system, this can only be done with doctor approval, and can result in discipline for the nurse if their assessment is incorrect. The RN was therefore placed in the difficult situation of either risking her job or performing a treatment protocol that she believed was unnecessary and could put the patient at an increased risk of harm.

NNU survey findings reveal deep problems with the use of algorithms in health care. (See Attachment 2 for a summary of these findings.) NNU surveyed registered nurses about their

---


experiences with algorithms in 2021. Out of 795 RNs who responded to the relevant questions, 172 respondents (21.6%) said they were not allowed to “override clinical practice guidelines, clinical pathways, or electronic or computer-based tools that [they] believe are not in the best interest of the patient”, 200 respondents (25.2%) could only do so with the approval of a doctor or supervisor, and 204 respondents (25.7%) did not even know if they were allowed to override the recommendations. Only 117 respondents (14.7%) were allowed to override algorithms based on their own judgment. The fact that a majority of registered nurses who responded cannot override or do not know if they can override algorithms is concerning because 246 (31.0%) said they had been “been prompted by a clinical practice guideline, clinical pathway, or electronic or computer-based tool to make choices about patient care, patient care staffing, or other clinical issues that [they] believed were not in the best interest of the patient based on [their] clinical judgment and scope of practice.”

As AWSM systems become increasingly pervasive, RNs professional judgment may atrophy, and RNs may lose the ability to exercise their professional in situations where AWSM technology cannot do so. Assessing patients and developing a nursing care plan is a skill, grounded in education and professional judgment, which must be maintained and exercised, or it may be lost. Indeed, it is for this reason that clinical experience is a key requirement to become licensed as an RN. Removing opportunities to exercise professional judgment and maintain these skills will leave RNs and patients with limited recourse in circumstances where the system is ineffective.

In sum, health care employers seek to minimize nursing judgment from the provision of health care and use AWSM and HIT technologies to shift patient care to others in order to reduce labor costs. However, the law requires that certain health care duties legally be performed by a licensed RN precisely because the license indicates that they have sufficient knowledge, experience, and judgment to safely manage those responsibilities. RNs are left with the legal and ethical responsibility to care and advocate for their patients but without the time, autonomy, or information they need to do so safely. Health care employers are actively lobbying to change statutes and regulations to enable this shift. They have been utilizing the industry-created RN staffing crisis to justify these changes, dramatically degrading the quality of care provided at US health care facilities.

OSTP must ensure that all federal regulators understand that AWSM technology cannot safely or ethically replace the exercise of judgment by a professional. Policies adopted to regulate AWSM technology at health care facilities must prevent the routinization of core nursing tasks that results in the deskilling and of nurses and the erosion of nursing judgment.

h. Whether you (or, if relevant, your representative, like a labor union) have any visibility into the data collected on you or how it is used, including whether data on you collected by surveillance can be shared with other companies, trade groups, or third parties;
As discussed in NNU’s response to questions 1.c., 1.e., and 1.f., health care employers often fail to notify NNU or its members when new AWSM technology is being implemented in the workplace, taking the position that these are simply updates of older, “dumber” technology, and within their management rights to implement without notice to the union or an opportunity to bargain. Likewise, management rarely provides information about what new data is being collected and how this data is being used. To the extent the NNU or its members have had any knowledge, input or control over how, where, and over what automated surveillance occurs, this has been the result of aggressive collective bargaining by the union, and the diligent work of its members in worker committees, comparing output data and drawing statistical conclusions. NNU and its members are not provided the same information as the employer about how this system works or how it will be implemented. Typically, they are merely presented with the introduction of AWSM technologies as a fait accompli and may be given an opportunity to bargain over the effects of its implementation.

While nurses have some sense of how this data is being used when they must interact with these systems as part of providing care, such as knowing that EHR information and metadata is being used to determine acuity levels and staffing requirements, they have no insight into whether the data is also being shared with other companies, trade groups, or third parties. The risk that such data sharing may be taking place only serves to amplify the clinical, collective bargaining, nursing practice and privacy concerns highlighted in this RFI response. Also, somewhat unique to the health care setting, the sharing of data might implicate the Health Insurance Privacy and Portability Act, which has strict rules about maintaining the privacy of patient health information.

Furthermore, as discussed throughout this comment, RNs and other clinicians typically have no way of knowing how the data being collected is being used to make and inform clinical decisions, such as acuity determinations and nursing care plans. Indeed, no one, including the designers of the AWSM systems themselves, may know precisely how this information is being used if it is processed through a machine-learning algorithm or similar AI technology. This prevents nurses from double checking these systems to ensure they have reached the correct conclusion. This also prevents RNs maintaining and exercising the nursing skills and professional judgment to make these determinations without relying on AWSM technology. The lack of transparency about how AWSM data is being used thus has important clinical implications for the practice of nursing as well. OSTP must therefore demand complete transparency regarding the operation of these systems before they are implemented in health care workplaces.

**1. How the use of automated surveillance and management systems has changed how you do your job or how your employer treated you at your job:**

The use of AWSM systems has greatly impacted how RNs do their jobs. Health care employers use AWSM systems to undermine use of skill and judgment by registered nurses, as discussed in
section g. and throughout this response, and to support new models of health care, like so-called hospital-at-home programs and gig nurse staffing platforms, which put patients in danger and degrade RNs’ terms and conditions of employment. Employers aims include replacing RNs at the bedside and instead having them lead patient care teams, often remotely, and/or making periodic virtual visits of patients.

(1) AWSM systems are the basis for new, problematic health care delivery models that put RNs and patients at risk in order to maximize corporate profits, such as hospital-at-home models, telehealth, and gig-nurse staffing models.

AWSM technology supports and facilitates the proliferation of dangerous new care models such as hospital-at-home programs for acute “in-patient” care, telehealth, and gig-nursing. Hospital-at-home uses patient monitoring and communications technology to facilitate leaving patients in need of acute hospital care in their homes with limited visits from health care professionals. The proliferation of telehealth models where nurses counsel patients remotely enable nurse-patient interactions to be tracked closely, facilitates nurses being penalized based on tracking metrics, and undermines safe patient care. Gig nurse staffing platforms manage RN staffing by algorithm. They take advantage of the ability of technology platforms to plug nurses into individual shifts to move away from care models where experienced, consistent, nursing care is provided in environments familiar to them, supporting their ability to provide safe patient care. In contrast, with gig staffing, nurses with limited orientation or unit-specific expertise are expected to care for patients in unfamiliar facilities.

These schemes seek to dramatically lower labor costs by replacing hands-on skilled hospital care with technology, gadgets, contract workers, and free labor by family caregivers and patients. The shift to acute hospital care in the home and telehealth also improves profits for health care employers by eliminating their overhead expenses related to building, running, and maintaining a hospital. .

However, as described below, these programs are dangerous for patients and undermine working conditions and employment protections for nurses.

(2) AWSM technology and ambient intelligence-based monitoring systems support hospital-at-home models, degrading the ability of RNs to provide safe patient care, increasing the acuity of patients in hospitals, and threatening to increase hospital closures and lead to the loss of jobs.

The emergence of AWSM technology has enabled the alarming growth of hospital-at-home programs for acute “in-patient” care. Instead of admitting patients in need of acute inpatient care, who would otherwise be traditionally hospitalized, they are sent home with patient monitoring technology, including visual, audio, and biometric monitoring devices, to be “admitted” for “hospital care” at their home. The patient is told a team of medical professionals will monitor
them remotely from a medical hub. These hubs could be many miles away, or even in a different state, from the patient. Staff is sent out to check on the patient as the need arises.

(a) AWSM technology combined with pandemic-era crisis standards of care has led to increased use of hospital-at-home models.

NNU’s response in this section largely focuses on the CMS Acute Hospital Care at Home (AHCaH) program. (For additional information, see Attachment 3, National Nurses United’s September 2022 Report “Medicare’s Hospital at Home Program is Dangerous for Patients.”)

The growth and development of AWSM technology enabled initial acute hospital care at home programs funded by both public and private insurers and health maintenance organizations (HMOs). However, the rapid growth in hospital-at-home programs was supported by waivers to certain conditions of participation in the Medicare and Medicaid programs implemented in the early months of the Covid-19 pandemic. Specifically, the U.S. Centers for Medicare and Medicaid Services (CMS), through AHCaH program, waived certain CMS Hospital Conditions of Participation, including a key provision which requires “nursing services to be provided on premises 24 hours a day, seven days a week and the immediate availability of a registered nurse for care of any patient.”63 These waivers have been extended by statute through the end of 2024. While programs providing acute, inpatient-level hospital care in the home existed previously, the CMS waivers enabled the rapid growth of these models. As of a June 16, 2023, update, CMS lists 283 hospitals run by 125 systems in 37 states that have current CMS waivers to run these AHCaH programs.64

In an emergency, patients in a fully operational hospital can be treated immediately under CMS’s 24-hour nursing services requirement for acute care facilities. But for patients being treated at home, CMS only requires an emergency response to a patient’s home within 30 minutes. From there, a patient may need to be transported to a hospital, a process that can further delay lifesaving care. Moreover, after a doctor performs an initial medical history and physical exam for an AHCaH patient, CMS does not require any additional in-person registered nurse or doctor visits with the patient. Instead, the AHCaH program requires just two in-person patient visits a day by an RN or community paramedic. Thus, through this program, hospitals are able to receive full reimbursement at inpatient rates for “treating” patients in their homes, despite not providing nearly the same level of nursing coverage or care.

As a result, the AHCaH program allows hospitals to drastically reduce labor and overhead costs by pushing patients out of the hospital, while still collecting the same reimbursement rates from CMS. This, in turn, increases profits for hospital employers. At the same time however, this


greatly decreases the quality of care received by these patients, as they no longer have access to the equipment, medical resources, and regular in-person evaluations by licensed RNs. Instead, many of the duties previous performed by RNs are shifted to untrained and inexperienced relatives or partners and are unqualified to identify and respond to the myriad of health emergencies that may arise when treating a patient in need of acute care. In some cases, patients may be in their homes alone.

(b) **Hospital-at-home models impact workers and endanger patients by increasing the acuity of patients in hospitals.**

Treating patients needing acute inpatient-level care in their home degrades the quality of care received by patients from what typically received at hospitals. The AHCaH program hurts nurses by shifting work previously performed by them in hospitals to untrained volunteers. It also allows hospitals to move patients with less severe conditions outside of the hospital, increasing the average acuity of patients in the hospital and the workloads of nurses working within the hospital.

The AHCaH program and similar programs do not and cannot provide patients with the ongoing, in-person assessment and treatment by RNs and other health care professionals that acute care requires. Although the bulk of patient care in hospitals is provided by registered nurses, hospitals employ a wide variety of health care professionals who are readily available 24 hours a day, including doctors, respiratory therapists, and pharmacists. Within the inpatient hospital setting, RNs and other health care professionals are able to draw on the collective experience of nursing, medical, pharmaceutical, and other staff. This knowledge base is lost when a patient’s care is shifted to the home and a patient’s family may be required to provide this care with limited outside support. Some hospitals currently participating in the AHCaH program do not require another person to be present in the home. Instead, they may leave the patient alone for long stretches of time or provide intermittent support from home health aides to supplement the twice daily visits from an RN or community paramedic.

RN’s are particularly concerned about what will happen to AHCaH patients when they code. A patient’s condition can go from bad to life threatening in just minutes. However, the AHCaH program only requires an emergency response within 30 minutes rather than requiring that an emergency response be available immediately. Without immediate attention from health care professionals and access to necessary treatment resources, patient morbidity and mortality rates increase. In contrast to the AHCaH program, most acute care hospitals have trained and certified staff readily available to respond to emergencies. These emergency response teams most often consist of an RN and a respiratory therapist, as well as either a physician, an

---


advanced practice registered nurse, or a physician assistant.\textsuperscript{67} It is the registered nurse, based on the regular monitoring and assessing of patient status, who most often initiates the rapid response emergency code. Delaying emergency response by 15 minutes or more is shown to increase the likelihood of intensive care unit admission or death in a variety of conditions.\textsuperscript{68}

Our members have already seen the serious consequences of trying to replace acute, inpatient-level hospital care performed by experienced RNs and other health care professionals with home care performed largely by the patient and their family members. One member reported seeing Covid patients who were sent home with an iPad and other monitoring equipment return to the emergency department with oxygen levels “so low their lips were blue, and they needed immediate lifesaving interventions,” and another patient was returned to the hospital by ambulance “with a dangerously high fever resulting from a serious infection and was nearly septic.”\textsuperscript{69}

In sum, acute, inpatient-level care at home, without the resources available at a hospital, including 24-hour nursing care, is simply inferior to traditional care in a hospital at preventing negative patient outcomes. RNs see it as depriving patients of professional, 24/7 nursing care, with the most vulnerable, least resourced, and often Black, Indigenous, Brown, and other patients of color and their households suffering the worst outcomes and perhaps death. Nurses at the bedside in hospitals are put at risk as hospitals use the reduction in patients to justify reducing RN staffing, while simultaneously increasing average patient acuity.

\textbf{(c) Acute-hospital-care-at-home programs shift nursing care to family members, burdening unpaid caregivers, taking work from skilled professionals, and putting patients in danger.}

With no in-person professional nursing staff available 24/7 in patient homes, the burden of care inevitably falls upon members of the patient’s immediate household -- typically family members with no medical education, knowledge, or training. Caring for a patient at home puts enormous strain on the entire household, especially the caregivers who are very often the women, who must balance jobs, childcare, and other responsibilities with the enormous burden of providing acute medical care.

In addition, the idea that family members can provide hospital-level care is absurd and unsafe. Registered nurses often serve as the last line of defense for patients against medical errors, especially in the area of medication administration. RNs receive significant training on passing,\textsuperscript{67} Mitchell OJL, Motschwiller CW, Horowitz JM, Friedman OA, Nichol G, Evans LE, Mukherjee V. Rapid Response and Cardiac Arrest Teams: A Descriptive Analysis of 103 American Hospitals. Crit Care Explor. 2019 Aug 7;1(8):e0031. doi: 10.1097/CCE.0000000000000031. PMID: 32166272; PMCID: PMC7063949.


\textsuperscript{69} Berger, R. and Hwang, L., \textit{Don’t Try This At Home: The national hospital industry is peddling programs to treat acute-care patients in their residences, instead of in the hospital where they belong}. National Nurses United. \texttt{https://www.nationalnursesunited.org/article/dont-try-this-at-home}. Accessed June 28, 2023
handling, and wasting medication, and discipline for medication errors can be severe. Yet hospitals, such as UC Irvine Medical Center in Irvine, Calif., write in documents submitted to the state health department supporting its hospital-at-home program that patients and family/caregivers can give oral, subcutaneous, intramuscular, and even intravenous medications if they are assessed on their knowledge and skills. A remote RN is supposed to watch over video when oral medications are given and document the medication administration in the record. But this is a far cry from the level of protection offered when a RN is responsible for the handling and administration of medication and the patient is in a brick-and-mortar hospital with lifesaving equipment and rapid response teams. Likewise, adjustments in medication are often called for based on observations of the patient, such as the smell of the breath or the feel of their chest, which can be difficult, if not impossible, to recognize through remote monitoring. Placing these duties in the hands of a lay person with only remote nurse oversight is dangerous to the patient and unfair to the individual who must assume these time-consuming and intellectually and emotionally taxing duties. Reliance on unpaid caregiving puts an unfair burden on women, who are disproportionately forced to leave the paid workforce or otherwise sacrifice to provide that care.

(d) Hospital-at-home models supported by AWSM technology place unreasonable burdens on nurses and other providers providing care and will further exacerbate the nurse staffing crisis and lack of available hospital beds.

The new care models enabled by AWSM technology, particularly acute hospital care at home programs, have the potential to lead to hospital closures and the loss of permanent, unionized, nursing jobs. If acute hospital care at home programs are allowed to grow, hospitals will close at higher rates—especially small-to-medium and more rural facilities. Already, overall hospital bed capacity nationwide is declining, dropping from 1.5 million in 1975 to about 919,000 in 2019, according to the American Hospital Association and Statista. And as more and more patients are sent home, hospitals will use the lower patient census as justification to close inpatient beds and further cut RN staffing, exacerbating the closure of community hospitals. Brick-and-mortar rural hospitals, already an endangered species, may go extinct. These programs are designed to make hospitals appear less relevant for our communities, and to make it easier to close hospitals, especially those that don’t make money or serve a high proportion of patients without private insurance. However, if the pandemic has taught us anything, it is that we need more hospitals, beds, and experienced, qualified RNs, not fewer.

(2) AWSM systems promote the use of telehealth, removing nurses from the bedside and displacing hospitals and other in-patient care models in order to lower labor costs.

The most widespread form of remote RN care is telehealth, nursing care provided remotely through telecommunications technology, typically a phone or webcam equipped computer. This is happening for patients treated in brick-and-mortar hospitals as well as in the home. Such systems have long been in place, however recent changes in telecommunications technology have made it possible for data and metadata related to phone calls or videoconferences to be
recorded, coded, and algorithmically analyzed. This allows hospital employers to determine how much time a nurse spends with each patient, how many patients a nurse treats during their shift, and even, to some extent, the affect and emotional state of the nurse during the call, all without ever having to observe any of the interactions themselves.

However, as described above, there are numerous reasons why nursing care performed in person is far superior to nursing care provided over the phone or video. Likewise, just as algorithms making clinical and employment decisions in hospitals frequently make errors, so do algorithms coding and reviewing RN performance during these calls. Yet it is often unclear what led an algorithm to make a particular determination. Thus, it can be very difficult to prove that an employment decision related to nursing performance identified by an opaque algorithm is inappropriate and should be overturned.

Furthermore, RNs simply cannot do their jobs as effectively if they are unable to physically interact with their patients. As described in Section 1.c. and elsewhere in NNU’s responses, tell-tell signs as innocuous as the smell of a patient’s breath or skin tone can be crucial in leading an RN to order a life-saving intervention. If such a patient were merely seen via telehealth, this crucial information would likely be lost, and could result in a death that would have otherwise been prevented. Telehealth thus puts patients at risk and leads to the deskilling of nurses.

Likewise, sometimes the system itself forms a barrier to the effective provision of nursing care. For instance, as recounted in a recent article in the Wall Street Journal, one member who worked in a call center as an advice nurse for a large California-based health system was prevented from recommending the care that she thought was appropriate because the system had no option for her to do so.70 Nurses at this call center use algorithms to categorize the illness of the caller, which involves entering information into a drop-down menu based on patient’s symptoms. When a patient called complaining of cough, chest pains, and fever, the nurse began processing the call through the cough/cold and flu algorithm. However, this algorithm did not provide an option for recommending an emergency room or doctor visit “unless the patient was spitting up at least 2 tsp of frank [visible] blood.”71 The nurse therefore only advised a phone appointment with a doctor several hours later. Tragically, the patient was later diagnosed with pneumonia, acute respiratory failure and renal failure and died several days later. In reviewing the case, an arbitrator correctly determined that the nurse was “pressured by this policy” and “viewed it as a directive,” and therefore ordered the health system to pay 3 million dollars in damages. Nevertheless, the nurse was also held responsible.72 This sad and unnecessary episode is a powerful example of how reliance on AWSM technology, particularly as a substitute for nursing skills and judgement, can be extremely dangerous to both nurses and their patients.

71 Ibid.
72 Ibid.
Telehealth is no replacement for direct, hands-on patient care by an experienced RN. While such systems have been in use in a limited capacity for years, advancements in AWSM technologies that support telehealth have resulted in it becoming increasingly widespread. In regulating AWSM technology, the federal government should ensure that it also regulates problematic new health care models, such as telehealth and remote patient monitoring, to ensure that their use does not degrade overall standards of care for patients and subject nurses to opaque and unfair performance measurement systems.

(3) AWSM systems support gig nurse staffing models, which results in the loss of workplace and labor rights for nurses.

Health care employers also use the data from AWSM systems to undermine wages and working conditions for workers through the use of gig RN staffing models. Gig work platforms enable the use of detailed information on worker activity and the pay that workers will accept to find the lowest pay level possible and to undermine worker power and organizing. Health care employers are increasingly using RN staffing platforms to improve their bottom lines.

Gig work is self-scheduled work, usually through a digital platform or app. Uber, Lyft, Door Dash, and similar tech companies use this model to employ workers. It is a highly exploitative work model in which employees are often misclassified as independent contractors, and thereby deprived of many workplace benefits and protections, including overtime, workers’ compensation, paid sick days, paid family leave, health and safety protections, discrimination and sexual harassment protection, health and unemployment insurance guarantees, and labor rights. This allows health care employers to dramatically decrease labor overhead costs and thereby increase profits, with little regard for nurses or patients.

Uber, Lyft, and Door Dash are already violating worker rights by misclassifying drivers as independent contractors, which shifts the costs normally borne by the employer onto the worker and prevents workers from organizing. Now health care Big Tech investors and employers are stepping up efforts across the country to misclassify RNs so they can increase their profits and undermine collective power. CareRev and ShiftKey are two examples of platforms and apps already drawing RNs into gig work, with many more anticipated.

One RN with ten years of experience working at an acute care hospital in Missouri reported that her hospital’s use of CareRev to provide additional RNs during the Covid-19 pandemic resulted in full time nurses becoming overburdened. Since the outset of the Covid-19 pandemic, the hospital was operating with fewer nurses and was filling this gap with travel nurses. While the exact timing is unclear because the hospital never provided notice to nurses or their union, around the summer of 2021, the hospital began using CareRev to provide per diem nurses in addition to travel nurses, who typically have multi-week contracts.

CareRev is an app-based platform, where nurses sign up, click boxes indicating their competencies, and are added to a pool of nurses who can then be assigned to hospitals that have...
contracted to use the application. Prior to working at the hospital, CareRev RNs are required to complete a one-day orientation demonstrating that they were familiar with the physical layout of the facility. Once this is completed, a nurse can see available shifts on the application and sign up for those shifts up to two hours before the shifts start. Nurses using the application were also permitted to cancel a shift they had selected up to 30 minutes prior to the start of the shift. The rate of pay for each shift is dynamic and based on demand in the same way as Uber or Lyft, with rates going up the closer it gets to the start of the unfilled shift. The rates are also generally higher than those provided to full-time staff, such that a full-time RN with nine years of experience makes roughly $35 per hour, whereas CareRev nurses started out making as much as $120 per hour. While this was later reduced to $80 per hour, and then to $60 per hour, it is still considerably more than the hospital’s regular RN employees. Moreover, many of the RNs hired at this rate through CareRev were new graduates, who had considerably less experience than the hospital’s staff RNs.

Not surprisingly, issues started to arise immediately. The application allowed CareRev nurses, through no fault of their own, to be placed in a given department (for instance, the Ear, Nose, and Throat (ENT) Department) without also indicating whether they were qualified and willing to do the work that was required in that department (such as performing and managing tracheotomies in the ENT Department). As a result, the more experienced nurses were required to take on the more difficult, higher acuity patients at a higher rate than was safe or appropriate, and to provide on-the-job training to CareRev nurses.

Using CareRev also complicated work performed by RNs who were regular hospital employees by making scheduling even less predictable than usual. That is, because CareRev nurses can cancel their shift up to thirty minutes before it starts, nurses employed by the hospital are often unaware how many CareRev nurses will actually show up the next morning. This puts a greater burden on the regular staff, who must pick up the slack. Moreover, this cycle was self-perpetuating. Nurses who previously worked as regular hospital employees increasingly began to quit those jobs and sign up for CareRev, knowing they could double their pay and gain greater flexibility while likely working for the same facility, treating the same patients. This then caused greater unpredictability and increased workload for nurses who were regular hospital employees, incentivizing them to move to gig work as well.

As this case study demonstrates, a gig-work model deprives workers of important workplace rights and degrades patient care as gig nurses often lack familiarity with the patient population and the facility. Moreover, the automated management algorithms that underpin gig work are designed to extract profit as a middleman between health care facilities and RNs. They do not and cannot safely manage RN patient care assignments.

j. Whether your employer has used information from an automated surveillance and management system in support of any discipline against you—and if so, what the action was, how and when you were informed, and what information was provided to you or your representative (such as a labor union):
Employers have used data from ASWM technology to support allegations of misconduct, despite the unreliability of this data and its inability to include the full context of employee actions. Employers also may use it to prompt discipline without informing employees. Employers have also disciplined nurses for failure to comply with recommendations made by AWSM technology, which dangerously undermines the crucial role of a RNs as patient advocates.

The nature of AWSM technology, which allows it to generate a dynamic, real-time account of employee activities within a health care facility, means that surveillance can be constant, and employers may act on information learned through surveillance without notifying employees or their unions. Employers may be using AWSM technology to take adverse action against nurses for engaging in protected activity using information gathered through AWSM technology without explicitly identifying AWSM technology as the basis for the adverse action.

Moreover, AWSM technology is often inappropriately used as the primary evidence to corroborate allegations of misconduct made by management. For example, one member who was accused of taking an extended break period by management was presented with a digital rendering, apparently drawn from several different AWSM sources, indicated that she entered and left the department at a given time. Significantly, however, this evidence did not rule out the possibility that she remained outside the department for a legitimate purpose other than taking a break, or that she simply misplaced her RFID badge or communication device, and the system was therefore misinterpreting her location. Even more concerning, there was no way to tell if the AWSM technology was simply malfunctioning. The fact that these systems are often opaque with respect to how they reach the conclusions they draw is a strong reason why using AWSM technology should not be used as the sole or primary basis for discipline.

Furthermore, the threat of discipline for questioning assessments and decisions made by AWSM technology is drastically undermining the profession of nursing by preventing nurse from learning, developing, and practicing core nursing skills that are essential for providing high quality nursing care. As described throughout this comment, AWSM technology is increasingly being used to make clinical decisions, such as acuity determination and nursing care plans directly. While nurses typically have the authority to override the clinical decisions AWSM technology makes, they may be subject to discipline if they attempt to do so, and a doctor or nurse supervisor disagrees with their determination. This threat of discipline for performing a core nursing task—ensuring that the nursing care plan and overall treatment of the patient are appropriate—is extremely disruptive to the practice of nursing. It discourages nurses from developing the skills to make these determinations on their own, and, in turn, leaves nurses unprepared to override the system when it makes a faulty determination or to step in if the system fails completely.

k. How automated surveillance and management has affected you—whether positively or negatively—including any economic, safety, physical, mental, and emotional impacts;
The use of AWSM systems has had substantial impacts on the nursing profession. Health care management uses AWSM systems to undermine the use of skill and judgment by registered nurses and to support new models of health care, like so-called acute hospital care at home programs and gig nurse staffing platforms, which put patients in danger and degrade RNs’ terms and conditions of employment. In the long-term, these changes are likely to have economic consequences as lower-cost labor replaces RNs and RNs transition into new roles. The health care industry has created the staffing crisis that it is using to justify these changes instead prioritizing patient care and providing safe workplaces that keep RNs at the bedside.74

In the short-term, nurses face safety, physical, mental, and emotional impacts as the reliance on AWSM technology creates unrealistic and unsafe standards with respect to work speed and intensification and increased patient load. It is well established that high workloads and pressure to work faster are associated with adverse patient events, errors of omission, job dissatisfaction, and increased patient mortality.75 Despite this, hospitals and health care providers are constantly searching for mechanisms to maximize the number of patients served without increasing payroll. AWSM technology allows them to accomplish this by shifting duties previously performed by humans to monitoring systems. However, as described above, these systems are prone to errors which can be difficult for clinicians to recognize and prevent. Likewise, these errors can have a dramatic impact on patient care. (See Attachment 4, National Nurses United Comments to AHRQ on Use of Clinical Algorithms That Have the Potential To Introduce Racial/Ethnic Bias Into Healthcare Delivery, for in-depth discussion of issues with clinical algorithms.)

The problem of reliance on AWSM technology and algorithmic management systems in health care settings is exacerbated when a hospital or health system uses an average as a benchmark for clinical performance. When AWSM technology is used to establish clinical benchmarks, RNs and other clinicians are pressured to increase patient “throughput”. However, that pressure endangers patients who may take longer to care for in the emergency department or operating room or need a longer hospital stay.

In addition to work intensification, health care employers are using AWSM technology to promote what it refers to as “working at top of license,” a practice in which professionals are encouraged to only focus on the most advanced practices that their license permits. A necessary

---


and unspoken corollary of this principal, however, is that nurses are encouraged to spend less time with patients, leaving tasks such as checking on the patient, helping with ambulation, and other important care responsibilities to unlicensed staff. This prevents nurses from developing the rapport with their patients and deprives them of opportunities to observe their patient and understand their clinical needs and personal idiosyncrasies. As described throughout this comment, nurses play an integral role in making treatment and care decisions and are often the main point of contact and intermediary between the patient and the health system. “Working at top of license” is an attempt to remove them from this role and replace them with lower cost labor. This, however, will result in worse patient outcomes, as nurses will not have sufficient familiarity and rapport with their patients to recognize the tell-tale signs that often indicate that drastic changes in a nursing care plan or acuity determination are necessary. Likewise, taking nurses away from the bedside prevents them from developing the skills to recognize such signs, and to apply nursing judgment to determine the best clinical path forward. Thus, while “working at top of license” might seem like a benign policy designed to increase efficiency, in reality it will have a drastic effect on health care by removing nurses as the primary intermediary and point of contact for patients, and thereby preventing them from using and developing nursing skills and judgment that are necessary to be responsive to patients’ needs and form an effective care plan.

l. How automated surveillance and management systems have affected your workplace rights, including rights around collective action, labor organizing, collective bargaining, pay, reasonable accommodations, health and safety, discrimination, and harassment—or your expectation of retaliation when exercising these rights;

See NNU’s responses to questions l.d., l.e., l.f., and l.j.

m. How these systems have impacted your non-working hours, personal time, or the privacy of other members of your household;

AWSM technology clearly interferes with the personal time and privacy of nurses while they are on break or in private spaces at the facility. As described above, AWSM technology allows comprehensive tracking of almost all nurse movement and activity at the health care facilities where it is implemented. This includes during nonwork times, such as breaks, when management has no legitimate basis for tracking the movements, activities, and conversations of its employees. Movement tracking also covers nonwork spaces that used to be important venues for engaging in protected activity, such as break rooms and parking lots. While these spaces were originally available to confer with other nurse about terms and conditions of employment, mistreatment by supervisors, dangerous working conditions, and other matters free from the interference or oversight of management, this is no longer the case, as nurses correctly assume that they are being surveilled and monitored electronically through AWSM technology. This, in turn, chills the exercise of those protected rights.
Furthermore, by implementing this technology without explaining to nurses or their representatives the full extent of its capabilities and how it works, health care employers create the impression of near constant and total surveillance, even outside of work hours and workspaces, even if the AWSM technology implemented by the employer does not actually have this capability. For instance, a nurse likely does not know which of the devices they carry are being used to track their movements and record their conversations and may very well assume they are bringing at least some of this technology home with them, either in the RFID badges, their communications devices, or even their uniforms. This impression of surveillance leads nurses to alter their behavior outside of work hours as well, as they never know when or how the boss might be listening.

In sum, the ubiquitous nature of AWSM technology almost inherently leads to nurses being surveilled and monitored whenever they are at the facility, even outside of work time and in private spaces, such as breakrooms, bathrooms, and parking lots. Moreover, the opaque nature of this technology, and employers’ frequent practice of refusing to provide notice, information, and an opportunity to bargain prior to implementation, exacerbate this problem by causing the impression of surveillance to extend outside of the facility as well, to all aspects of nurses’ lives.

To protect employee privacy, personal time, and personal space, the federal government must require that employers make clear the capabilities of AWSM technology, provide an explanation of how it can be used to track and monitor nurses, and engage in meaningful bargaining with the employees about whether and how such technology is be implemented.

p. Whether you work for an employer that receives Federal funds (for instance, as a Federal contractor).

The vast majority of NNU members, potentially all of them, work for a health care provider that receives federal funds, particularly funds for Medicare and Medicaid programs.
GENERAL COMMENT

See attached file(s)

ATTACHMENTS

2023-06-29 Athena OSTP Comment
Before the
White House
Office of Science and Technology Policy

In the Matter of
Automated Worker Surveillance and Management
Document Num. 2023-09353

Comments of
Athena Coalition

&

AI Now Institute
The Awod Center
Center for Popular Democracy
Center on Privacy & Technology at Georgetown Law
Demand Progress Education Fund
For the Many
Human Impact Partners
Jobs With Justice
Missouri Workers Center
National Black Worker Center
Make the Road New Jersey
OLE
Turkopticon
United for Respect
Warehouse Worker Resource Center

Filed June 29, 2022

Ryan Gerety
Acting Director, Athena
Table of Contents

Overview: the Biden-Harris administration can stand with working people and stop corporations like Amazon from using automated surveillance and management to undermine worker safety and dignity............................................................................................................................................................ 3

I. Amazon uses automated surveillance and management to maximize control over warehouse workers and subcontracted drivers by dictating each task, monitoring each second, and imposing a constant threat of termination.................................................................................................................... 4

II. This low-road system of management has far-reaching consequences for working people, their families, and the public........................................................................................................................................ 7

A. Individual productivity monitoring is used to enforce a dangerous pace of work.................. 7

B. This punishing and punitive system intentionally results in high-turnover and job precarity. 9

C. Surveillance is being used punitively, rather than to create better working conditions........ 9

D. Surveillance is being used to retaliate against workers and undermine their protected rights to speak out and take collective action................................................................. 10

E. Amazon’s rigid and fractured system of remote human resources and dependence on automated control has meant workers with disabilities are not getting legally required accommodations........ 10

F. Worker surveillance disproportionately harms Black and brown workers.......................... 11

G. Surveillance, automated management, and monopoly control enable corporations to benefit from misclassification schemes and unlawful control of so-called independent contractors.................. 12

H. Corporations that use these low-road models of punishment, control, and surveillance create an unfair competitive advantage and a race to the bottom........................................................................ 12

I. Pervasive surveillance and automated control increase corporate profits on the backs of workers, by reducing wages and deskilling jobs....................................................................................................... 13

III. The White House must safeguard workers’ rights by preventing predatory surveillance and automated management practices and fixing the gaps in labor laws and enforcement that employers leverage using these tools................................................................. 13

A. Expand investigations into Amazon’s violations................................................................. 15

B. Establish interagency collaboration on both Amazon and on worker surveillance and automated management............................................................................................... 15

C. Update federal agency standards and enforcement............................................................. 15

D. Establish standards on the use of worker surveillance by federal contractors............... 16

Conclusion................................................................................................................................................... 16

Appendix I: Courtenay Brown Testimony before the Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth (2021)................................................................. 17

Appendix II: United for Respect Testimony to Senate Subcommittee on Promoting Competition and Economic Growth in the Technology Sector (2021)......................................................... 19

Appendix III: Amazon Worker Letter to Shareholders (2021).................................................. 22

Appendix IV: Joint Statement to Regulators and Electeds on Amazon Worker Surveillance (2021) 23

Appendix V: Joint Statement on Worker Surveillance (2020)................................................25

Appendix VI: Joint Statement on Silencing Whistleblowers in the Workplace (2020)................28

Appendix VII: Memo to the White House Task Force on Worker Voice (2021).........................30
Overview: the Biden-Harris administration can stand with working people and stop corporations like Amazon from using automated surveillance and management to undermine worker safety and dignity.

In its request for information, the White House Office of Science and Technology Policy (OSTP) seeks input from the public on “the prevalence, uses and purposes, and deployment of automated worker surveillance and management systems.” In this response, we describe the use of automated surveillance and management within Amazon warehousing and logistics, provide Amazon worker testimonies on the use and impacts of these management methods, outline requested remedies from workers and civil society, and include supplemental materials from workers and civil society organizations.

We focus on Amazon in this response because its model is at the heart of understanding how surveillance and automated management can be used by corporations to enrich themselves to the detriment of workers, their families, and communities. We also focus on Amazon because it uses a combination of surveillance, monopoly, and leverage over workers to defend and expand its power and wealth. If Amazon’s model is allowed to set the standard in warehousing, logistics, and beyond, it risks undermining working conditions and wages for all working people.

Over the past decade, Amazon has grown from a company with 88,400 workers to one with 1.54 million. 1 Amazon is now the second largest private employer in the United States, and relies on thousands more third-party contractors to complete its distribution network. 2 Recently, Amazon surpassed FedEx in parcel volume and is behind only UPS and the USPS in terms of American package delivery services. 3

Amazon grew its warehousing and logistics empire using automated surveillance and management to exert a dangerously high level of control over warehouse workers and delivery drivers. 4 This level of control enables Amazon to enforce a dangerous pace of work, undermine worker organizing, and benefit from offloading risks onto small businesses and delivery drivers. The result is an unsafe, retaliatory, discriminatory, and highly insecure workplace.

Amazon, like other corporations, uses this dangerous, surveillance-driven management model without consequence because our weak laws and enforcement enable it to do so. Corporations like Amazon are also emboldened by a political and economic system that has left over 20

---

million workers trapped in low-wage jobs. For years, Amazon workers have organized and advocated for lawmakers and regulators to address these gaps and protect their rights.

In response to this request for information, coalition worker organizations The Awood Center, Missouri Workers Center, and Warehouse Workers Resource Center submitted testimony on behalf of Amazon workers fighting for safe working conditions, including: Yesenia Barrera, Mohamed Farah Hassan, Khali Jama, and Jennifer Crane.

By listening to workers and aggressively targeting the worst offenders and practices, the Biden-Harris administration has the opportunity to stand with working people over corporate interests and address the ways surveillance and automated management are further eroding working conditions for low-wage workers.

We submit this response on behalf of our 50+ member organizations who are working together to break the dangerous stranglehold of Amazon over our democracy, economy, and planet. We cannot have a thriving economy or democracy when the most powerful corporations in the world profit, grow, and outcompete other businesses by finding innovative ways to exploit workers. When employers are allowed to rely on low-road labor practices, then workers, communities, and responsible businesses are undermined and left facing the consequences. Attached to the comment are documents reflecting years of advocacy against Amazon’s surveillance and automated management practices.

I. Amazon uses automated surveillance and management to maximize control over warehouse workers and subcontracted drivers by dictating each task, monitoring each second, and imposing a constant threat of termination.

Amazon warehouse workers and drivers have documented and confronted surveillance and automated management systems and their impacts. They have spoken to the media, elected officials, and regulators; organized with their colleagues; and held walkouts in order to raise the alarm and challenge these systems. Without these efforts, little would be understood about these systems and the devastating consequences of this management model.

Warehouse workers and delivery drivers have their tasks dictated at each moment, are constantly monitored, and threatened with termination when they cannot keep up with dangerous quotas. This is Amazon’s “big innovation” and competitive advantage: integrating totalizing control,
surveillance, and punishment to enforce a dangerous pace of work at a minimal cost—and then leveraging the high turnover from people being pushed out, injured, or fired to scale-down its workforce when demand is lower.

In Amazon warehouses, each task is dictated and timed by handheld scanners at every second. Though it varies from facility to facility and job to job, Amazon uses two kinds of quotas. It sets an individual rate for each shift, and it additionally measures any amount of time that it determines to be idle time, or time off task by using the times between scans. Workers in our coalition report that managers monitor these indicators and push workers to go faster through several means: verbal warnings, warnings communicated through the scanner, visual warnings on a station screen, printouts, and large screens of everyone’s rates for comparative purposes. The determination of off task is rigid and workers report that it is error-prone. Some workers even keep a diary of their day, so that they can explain any gaps. Over the course of shifts that can be 10 or 12 hours, this monitoring and discipline paired with a threat of termination drives workers at a dangerously high pace, often doing the same motion over and over again.

In designing the system which measures and monitors time off task and rate, Amazon did not take into account how workers complete tasks, time they may need to rest, any injuries or accommodations they need, how long it would take to find a restroom, pray, or get back from the cafeteria in warehouses that are dozens of times bigger than a football field. Workers report being continuously disciplined for time off task and risk being fired for failing to meet often undisclosed and inconsistent micro-quotas (how many seconds you have to do one task). These rates are not set to meet any ergonomic safety standard, and Amazon has reported in the past that it sets rates to what 75% of workers are meeting. This means that a quarter of workers constantly feel behind and will rush to keep up. Workers also report that rates are not consistent throughout the year.

Within Amazon’s last mile delivery operation, it uses surveillance and automated management to maintain control of delivery while outsourcing employment liability to small local Delivery Service Partners (DSPs). Although DSPs are supposed to be independent businesses, Amazon dictates the delivery routes, order of deliveries, productivity quotas, training, scheduling, and


Amazon also has a gig-style delivery program called \textit{Flex} that relies on individuals to sign up for delivery jobs on the Amazon Flex app and deliver packages using their own vehicles. Even as so-called “independent contractors,” Flex drivers face substantial monitoring and surveillance by Amazon through the Flex app, as well as by customers who use home doorbell cameras to instruct workers and report on their performance.\footnote{Aiha Nguyen and Eve Zelickson, \textit{At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers}, Data & Society Research Institute (Oct. 12, 2022), https://datasociety.net/library/at-the-digital-doorstep/.} In an investigative report, \textit{Bloomberg} spoke to \textit{Flex} drivers and a former manager and found that workers were subjected to a high degree of automated management and were at risk of termination by the app:

\begin{quote}
Stephen Normandin spent almost four years racing around Phoenix delivering packages as a contract driver for Amazon.com Inc. Then one day, he received an automated email. The algorithms tracking him had decided he wasn’t doing his job properly. The 63-year-old Army veteran was stunned. He’d been fired by a machine.\footnote{Spencer Soper, \textit{Fired by Bot at Amazon: ’It’s You Against the Machine,’} Bloomberg (June 28, 2021), https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out.}
\end{quote}

We see a similar set of problems with workers who get jobs on Amazon’s Mechanical Turk, a platform for finding and getting paid for small tasks by anyone who posts a job. Over the last several years, Mechanical Turk workers have detailed problems on the platform and advocated for solutions. Amazon develops machine learning supervision of workers by using feedback from job posters, who have incentives and unchecked power to punish workers for unsatisfactory work. Job posters can withhold pay for work they do not like or understand and this, in turn, lowers workers’ ratings. Amazon also rates workers by subjecting them to hidden tests and comparing their answers to other workers.\footnote{Brian McInnis, Dan Cosley, Chaebong Nam, and Gilly Leshed. "Taking a HIT: Designing around rejection, mistrust, risk, and workers' experiences in Amazon Mechanical Turk." In Proceedings of the 2016 CHI conference on human factors in computing systems, pp. 2271-2282. 2016; Lilly Irani. “Algorithms of Suspicion: Authentication and Distrust on the Amazon Mechanical Turk Platform.” https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4482508} Employers often fail to train workers to produce the kinds of results they want, and offer no pathways for workers to repair mistakes or misunderstandings. Workers lack formal processes for contesting these evaluations and associated wage theft.
Amazon then uses this data collection to develop machine learning models that guess whether a worker is a “bad actor.” Workers flagged by machine learning find themselves locked out of their accounts with no explanation. One worker lost her account and access to her earnings, stored on the platform, for two weeks over what Amazon later admitted was a machine learning glitch. The machine learning detected two people – her and her son, it turned out – logged in and working on the same wifi network. The algorithm had “learned” that low quality workers shared wifi and flagged the account. On her suspension, the worker appealed to Amazon but got no response until Turkopticon, a Turk worker organization, approached Amazon collectively. Only then did Amazon re-investigate and admit that it made a mistake. An analysis of Amazon patents reveals that Amazon uses a surveillance of a wide range of behaviors to decide whether to trust the worker logged in behind the screen or to suspend them, without ever meeting the person or having a conversation.19

II. This low-road system of management has far-reaching consequences for working people, their families, and the public.

This level of monitoring and control at Amazon has no place in our economy. Corporate employers say that these technologies make workplaces more efficient and are necessary to be competitive, but those claims do not hold up to scrutiny. Instead, we find:

A. Individual productivity monitoring is used to enforce a dangerous pace of work.

By pairing task-to-task control, constant monitoring, and a threat of termination, Amazon enforces an unsafe pace of work where workers have little autonomy or ability to work safely, which is why Amazon’s injury rate is twice as high20 21 as the industry average.22 To avoid discipline, workers may forgo breaks and put aside safety procedures. Workers have repeatedly said that the pace of work is too fast and requires repetitive motions that create injuries over long shifts. The data indicates that injury rates are higher in the robotic facilities, where workers are at

19 Irani, p. 12
an even higher risk for repetitive motion injuries. The costs of injury and burnout are offloaded to families and the workers compensation system, rather than being internalized by the company. Unprecedented investigations by OSHA and the Washington State Department of Labor and Industries have substantiated these findings.

In March of 2022, Washington State Department of Labor and Industries found that Amazon willfully violated workplace safety laws, and the agency cited Amazon’s unsafe pace of work enforced through electronic monitoring. Willful violations are ones where the employer “purposefully disregard[ed]” or “acted with plain indifference to employee safety”. This action was preceded by four other citations by the Washington State Department of Labor and Industries for unsafe working conditions at Amazon. The March 2022 citation found that:

> The employer did not make sure that employees were provided with a workplace free from recognized hazards at Amazon’s BFI4 Fulfillment Center in Kent, Washington. Upon inspection, it was found that employees are expected to maintain a very high pace of work. Information collected documented that pressure is put on workers to maintain that pace without adequate recovery time to reduce the risk of MSDs. There is a direct connection between Amazon’s employee monitoring and discipline systems and workplace musculoskeletal disorders (MSDs).

---


In addition to the dangerous impacts of excessive pressure, studies of other sectors have found that when workers have less control and autonomy in their jobs, their physical and mental health suffers – pointing to the dangers of automated management and reduced worker autonomy.

**B. This punishing and punitive system intentionally results in high-turnover and job precarity.**

Amazon workers report that colleagues rarely stay over six months. Through a combination of exhaustion, disciplinary pressure, and termination, Amazon has a turnover rate of 150%, or higher. Amazon’s management system was never designed to retain people, according to executives, and thus high turnover is built into their model. Turnover is so high that Amazon itself worries that it will churn through the entire workforce in some regions. The combination of automated management that directs workers task-to-task and constant tracking means that Amazon can integrate new workers at a low cost, dramatically reducing incentives for a company to retain workers.

**C. Surveillance is being used punitively, rather than to create better working conditions.**

Corporations are adopting new workplace technologies for the sole purpose of disciplining individual workers, even in areas where technology could be used to improve working conditions. When Amazon developed new technologies to determine if warehouse workers were within six feet of one another, they then immediately used this information to selectively discipline and then fire workers, rather than figuring out how to improve the ability of workers to distance. Similarly, while Amazon claims its surveillance of drivers is for safety purposes, that

---


31 Jason Del Rey, Leaked Amazon memo warns the company is running out of people to hire, Vox (June 17, 2022), https://www.vox.com/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance.


surveillance is turned against workers to discipline people for minor infractions.\textsuperscript{35} And, as described previously, workers on Amazon Mechanical Turk face automated evaluation systems that can deplatform workers and hold their earnings at any time and without recourse. Across the board, these punitive systems are designed for workers to fail.

\textbf{D. Surveillance is being used to retaliate against workers and undermine their protected rights to speak out and take collective action.}

With limitless surveillance at an employer’s fingertips, targeting a particular worker is trivial: Amazon can go through troves of data to find a pretextual or dubious reason to retaliate against someone who is organizing or speaking out.\textsuperscript{36} This corroborates the memo published by National Labor Relations Board General Counsel Jennifer Abruzzo on how surveillance can undermine workers’ rights protected by section 7 of the National Labor Relations Act.\textsuperscript{37} Additionally, surveillance of workers is not limited to the workplace, and it was recently reported that Amazon monitored private social media groups of Amazon Flex drivers,\textsuperscript{38} and tried to recruit intelligence analysts to investigate labor organizing activities.\textsuperscript{39} Surveillance-fueled retaliation also raises discrimination concerns, as Black workers are more likely to be fired and disciplined in retaliation for advocating for worker protection.\textsuperscript{40}

\textbf{E. Amazon’s rigid and fractured system of remote human resources and dependence on automated control has meant workers with disabilities are not getting legally required accommodations.}

\begin{itemize}
\item \textsuperscript{38} James Vincent and Alex Castro, \textit{Amazon is reportedly surveilling its Flex delivery drivers in private Facebook groups}, The Verge (Sep. 2, 2020), https://www.theverge.com/2020/9/2/21418057/amazon-surveilling-flex-delivery-drivers-facebook-groups-subreddits-strikes-protests.
\end{itemize}
Amazon’s automated management system does not provide sufficient flexibility for accommodations, a potential violation of the Americans with Disabilities Act. While the ADA requires an interactive process between employee and supervisor to determine reasonable workplace accommodations, Amazon’s productivity metrics and automatic disciplinary systems undermine this process. Workers have reported that Amazon does not give appropriate accommodations in a timely manner, as reasonable requests like weight limits and the need to occasionally sit down interfere with quotas. This becomes especially pernicious when considering the injury rate of longtime Amazon workers. Amazon has also been accused of using employees’ disability and accommodations requests as a means of retaliation for their workplace organizing activity, as alleged in the case of Jordan Flowers and Jennifer Bates.

**F. Worker surveillance disproportionately harms Black and brown workers.**

Due to systemic racism and discrimination, Black and brown workers are more likely to be in low-wage jobs, less likely to be listened to when they raise concerns, and more likely to face retaliation. Additionally, algorithmic decision-making can dramatically reinforce and exacerbate racial disparities, particularly where people impacted have no recourse or power. For many of these workers, the level of monitoring is akin to discriminatory police surveillance in their communities.

---


G. Surveillance, automated management, and monopoly control enable corporations to benefit from misclassification schemes and unlawful control of so-called independent contractors.

Amazon’s surveillance and management allows them to control third-party companies and individual independent contractors without providing those workers and businesses with either the protections of the traditional employment relationship or the benefits of true independent contracting. The intensity of control via vertical restraints and surveillance obliterates any distinction between "employee" and "independent contractor" that public agencies have relied on in the past. Meanwhile, these drivers are blocked from making claims on Amazon corporate headquarters for rights or resources or from collectively bargaining with their real bosses over their working conditions and compensation. It is no surprise that abysmal rates of workers getting hurt on the job and other indicators of worker misery are endemic to delivery at Amazon. And when Amazon's unreasonable delivery or delivery routing requirements lead to vehicle crashes, Amazon can claim that it bears no legal responsibility to the victims.

H. Corporations that use these low-road models of punishment, control, and surveillance create an unfair competitive advantage and a race to the bottom.

Amazon’s market size in shipping and retail, combined with the extremity of its unethical worker surveillance and automated management practices, further push competitors’ practices and related industry standards to deteriorate even for unionized workers, in an

---


56 Matt Day and Spencer Soper, Amazon Has Turned a Middle-Class Warehouse Career Into a McJob, Bloomberg (Dec. 17, 2020),
ever-intensifying race to the bottom for workers who are the most vulnerable to surveillance-fuelled abuse.

Widespread adoption of Amazon’s model also represents the private sector offloading its traditional responsibilities onto workers themselves and the public, with government funds subsidizing corporate exploitation through social welfare and health care programs shouldering the consequences of inhumane and injurious workplaces. By taking advantage of gaps in labor laws and enforcement, Amazon places its competitors at an unfair disadvantage to the detriment of everyone.  

I. Pervasive surveillance and automated control increase corporate profits on the backs of workers, by reducing wages and deskilling jobs.

While some technologies such as supermarket scanners allow companies to raise profits by using workers more efficiently, surveillance technologies raise profits by the cruder mechanism of increasing the pressure on workers. Additionally, by achieving the heightened degree of control that surveillance enables, employers have no need to pay higher wages to encourage extra effort. The supermarket scanner allows each worker to serve more customers with the same level of effort, but surveillance technologies can dangerously accelerate the pace of work. This method of technology-backed pressure and control that focuses on extraction rather than efficiency should be thought of as low-road innovation.

Aligned with the argument, studies show that Amazon is undercutting wages in the logistics industry. A Bloomberg investigation found that when Amazon opens new facilities, the average warehouse industry wages fall in that county. The same study found Amazon’s employee promotion rate to be far below that of the industry average, reflecting the high turnover rate and lack of advancement opportunities facing most associates.

III. The White House must safeguard workers’ rights by preventing predatory surveillance and automated management practices and fixing the gaps in labor laws and enforcement that employers leverage using these tools.

As the Biden-Harris administration examines this issue, it should consider a new generation of economic policies, labor rights, and enforcement actions in order to steer our economy away


from exploitative profit models that leverage workplace technologies to the detriment of working people and a competitive economy by taking the low road. A comprehensive approach will be necessary to directly address the technology, but just as importantly, to address the underlying gaps in worker rights that are enabling this disaster. In response to outcry from Amazon warehouse workers and drivers, state\textsuperscript{61} and federal lawmakers\textsuperscript{62} and agencies\textsuperscript{63} have already started taking action, but much more will be needed.

Amazon workers have raised an important set of issues for the administration to focus on: the ways surveillance and automated management enables new management models that maximize profits while reducing worker pay, increase injuries and reduce worker control, maximize employer flexibility through worker precarity, and facilitate retroactive searches for reasons to fire people who speak out and organize.

A central driver of these issues is the ability of the employer to constantly monitor, control, and discipline workers. While there are many ways to look at the potential harms of surveillance and automated management, and a growing number of specific technologies to examine, the case of Amazon points to this as a central imperative:

**Prevent continuous performance monitoring linked to adverse employment decisions such as formal or informal discipline, termination, pay, or promotions.** Amazon demonstrates that this type of monitoring puts too much power in the hands of the employer and will be abused to the detriment of workers, as described by the multiple harms detailed in the previous section. Union contracts that prevent this type of monitoring demonstrate that putting workers under the microscope is not necessary. Right now, corporations are using poor management practices like *time off task* and unsafe quotas to increase profits and beat out competitors, rather than investing in actual productivity innovations.

---


To begin to address this issue, we recommend the administration must:

**A. Expand investigations into Amazon’s violations.**

Expand investigations into the widespread and longstanding patterns of abusive and unethical practices at Amazon – including safety, disability discrimination, illegal retaliation, and misclassification – and address them as systemic, company-wide issues rather than one-off cases tied to specific individuals or facilities.

The Biden-Harris administration must continue to investigate safety violations at Amazon warehouses, and use OSHA’s already unprecedented investigations as an opportunity to examine the links between injuries, pace of work, and punitive surveillance. The administration should also investigate Amazon’s ADA violations with attention to the relationship between disability discrimination and rigid automated management systems. Similarly, the administration should examine potential unfair methods of competition violations in Amazon’s delivery system, which forces drivers into independent contractor positions, while maintaining complete control. These are critical opportunities to examine the impacts of these systems within one of the largest employers in the country.

**B. Establish interagency collaboration on both Amazon and on worker surveillance and automated management.**

Corporations like Amazon can outspend federal agencies tasked with regulating their conduct, and on top of that, each investigator in each agency is independently learning the complexities of Amazon’s management model. The same systems of surveillance and automated management are implicated in injuries, high turnover, discrimination, retaliation, unfair vertical restraints, and misclassification. Understanding these connections and the systems themselves would benefit from continued interagency collaboration specifically on Amazon, specifically, and on automated management and surveillance, generally. To facilitate interagency collaboration and establish a longer term agenda on workplace technology, we recommend the administration establish a division within the Department of Labor focused on workplace technology.

**C. Update federal agency standards and enforcement.**

As evidence mounts that employers are using surveillance and automated management in ways that create dangerous, retaliatory, and discriminatory workplaces, agencies should create new

---

standards that directly address these technologies as well as enabling conditions, which include: the pace of work, unfair vertical restraints, misclassification, joint employer accountability, and surveillance-enabled retaliation.

**D. Establish standards on the use of worker surveillance by federal contractors.**

To start, the federal government should not contract with corporations that have a record of violating health and safety laws enforced by OSHA, anti-retaliation laws enforced by the NLRA, or any other federal labor laws. Amazon, for example, has an established record of using surveillance and automated management in ways that violate these laws. Additionally, federal contractors should not be able to continuously monitor workers in ways that resemble *time off task* monitoring or use other technology practices that place workers in danger, are unnecessarily invasive, or violate the law.

**E. Support policies that counter worker surveillance and automated management, as well as address the gaps and loopholes that employers are exploiting with this technology.**

Additionally, the administration should work across agencies and with Congress to address existing gaps in worker protections that currently enable corporations to use these technological tools to maximize profit, leverage over workers, and gain market control. These policies include establishing a just cause standard for termination, standards for the use of technology in the workplace, strengthening the right to organize and establish a union, protections for temporary workers, and updating the definition of an employee and a joint employer to meet the modern employer practices and the uses of technology to establish worker control.

**Conclusion**

Amazon’s punitive and punishing model is a clear example of what needs to change: people should not fear being fired at every turn, subjected to constant disciplinary performance monitoring, retaliated against, or pushed until their bodies break. Enabling and even incentivizing these low-road practices is a policy choice that we have the opportunity to change. Amazon’s model is the current example of a long pattern of corporations being allowed to use monitoring and punishment, rather than better pay and benefits, to extract additional effort from workers. If these practices are not prevented and made illegal, we will see a continued race to the bottom to the detriment of the entire economy. The rapid development and deployment of workplace technology makes addressing these issues all the more urgent.

Establishing robust worker protections and rebalancing power between workers and employers would not only benefit hundreds of thousands of Amazon workers, but could reorient the economy and tech innovation toward more equitable and sustainable outcomes. In order to do

---

this, law, regulation, and enforcement should prioritize worker health and safety, protect against predatory surveillance and automated management practices like time off task, fortify the rights of workers to speak out and organize, guard against low-road business models, and incentivize innovation that enhances worker well-being and shared economic prosperity.

Appendix I: Courtenay Brown Testimony before the Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth (2021)

Remarks by

Courtenay Brown

United for Respect Leader

Testimony before the Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth

Public Hearing on: Promoting Competition and Economic Growth in the Technology Sector

Thank you for inviting me to share my experience with you today, Senator Warren and members of the committee. My name is Courtenay Brown and I live in Newark, New Jersey. I’m currently working at an Amazon fulfillment center and have been for four and a half years.

Before working at Amazon, I served my country as a service member in the U.S. Navy. I took seriously the commitment I made to my country then, and I take it seriously now as a Member Leader with United for Respect.

I’m here today, Senators, to raise the alarm about Amazon's business model because it’s a threat to working people and it’s a threat to our economy. 1 out of every 153 American workers is an Amazon employee and this multi-billion dollar corporation grew on the back of its workers by exploiting them. I’m looking to you to stand up to corporations like Amazon and protect us.

The job I do is a much-needed service, especially since the COVID-19 pandemic began. As a Process Guide, I sort 35,000-50,000 groceries daily for delivery to homes in New York City and New Jersey. I’m in and out of our cooler constantly, stepping in and out of temperatures as low as negative 10 degrees, and picking up and setting down items with little to no rest. The work I do is supposed to be done with 30-40 people but we are operating with 25 people or less. Because our work is so essential, we need more hands on deck, not less, so that we can take turns getting breaks and much-needed rest. But, Amazon does not retain its workers.

Amazon’s multi billion-dollar wealth is made possible by offering same day delivery and the corporation has achieved this speed and scale through sheer brutality — watching, timing, and punishing associates like me and my coworkers for not working fast enough and not allowing associates to take time off to adequately recover, rest, and prevent burn out.

From the moment we pull into the parking lot we are monitored. And If we fall behind in any way during our 11 hour shift, we risk being disciplined. We are pushed to our limit to the point where we can’t even take regular bathroom breaks. Often we have to run to and from the bathroom in under 2 minutes so we don’t get in trouble. On top of that, the bathrooms are gross and often broken.

The constant pressure and surveillance is why Amazon has twice the level of injuries and turnover compared to similar jobs. Research has shown that workplace injury rates are higher at Amazon facilities with more robotic and automated technology. I used to be a trainer and I saw firsthand how, out of 50 new hires, only 5 would make it to one or two months, and many quit soon after due to injuries and overexhaustion.

We are living in a country where machines are getting better treatment than people. The machines at my facility undergo routine maintenance checks to ensure they don’t burn out.

Yet the one time I needed time off to be with my family to recover from my mother’s passing, I was told I could only get two days off for bereavement. Two days to plan a funeral and process my mother’s death was not enough so I had to take a month off UNPAID because that’s the only option Amazon gave me. A month of UNPAID time off, while Jeff Bezos made $75 billion last year thanks to me and my coworkers.

Amazon’s high-tech sweatshop caused me to develop plantar fasciitis and tendonitis - a debilitating pain in my heel and ankles - because I’m having to stand for long periods of time at work with little to no rest. One time the burning sensation around my heels was so painful that I ended up in the emergency room. I begged the doctors not to keep me longer than a few hours because I had to go back to work. I was more concerned I’d get punished at work for calling out than prioritizing my own health.

This kind of exploitation isn’t just happening to me -- people have been working through the pandemic non stop because Amazon won’t let us take time off. Often we are so exhausted we break down and cry. And a coworker of mine had to stop pumping her breast milk at work after giving birth to her baby because she was not getting the support she needed. This is the type of work environment Amazon is perpetuating across the country.


Amazon Associates have been fighting back against these dangerous conditions for years. Instead of fixing the problem, Amazon is only doubling down on its exploitative model. Jeff Bezos himself recently told shareholders that he plans to use more automated control of workers in the warehouses.\(^69\)

The worst part of all is that Amazon is setting up its high-tech sweatshop in Black and Brown communities desperate for work. The pandemic has closed a lot of businesses in my area so even someone like me who has considered looking for another job -- I can’t because there are no jobs available or the pay isn’t enough to make rent and put food on the table.

This committee is considering competition and economic growth in the tech sector. When corporations write the rules to maximize their profit, they ensure they win by all means necessary -- including exploiting workers and gutting small businesses.

Senators -- I’m looking to you to stop corporations like Amazon from ruining our economy and dictating the workplace standards for hundreds of millions of workers like me. I’m asking you to help me put an end to inhumane, exploitative practices that leave America’s workers injured, exhausted, and mentally battered each day.

Our country needs elected officials to side with working people -- to side with essential workers -- not big corporations.

Thank you.

Appendix II: United for Respect Testimony to Senate Subcommittee on Promoting Competition and Economic Growth in the Technology Sector (2021)

**Public Hearing on: Promoting Competition and Economic Growth in the Technology Sector**

**United for Respect, December 2021**

We cannot have a thriving economy or democracy when the most powerful tech corporations in the world profit, grow, and outcompete small businesses by finding innovative ways to exploit working people. When success is the result of low-road labor practices, workers, communities, and responsible businesses are undermined and left facing the consequences.

Over the past decade, Amazon has grown from a company with 56,000 workers to one with 1.47 million.\(^70\)\(^71\) Amazon is now the second largest employer in the United States, and relies on thousands more third-party contractors to complete its distribution network.\(^72\) Today, Amazon dominates multiple markets and industries: it’s projected to capture 41.4% of U.S. retail e-commerce in 2021, 40.8% of the cloud computing market through Amazon Web Services, and 21% of the streaming market with Prime

---


\(^{70}\) https://s2.q4cdn.com/299287126/files/doc_financials/annual/269317_023_bnk.pdf

\(^{71}\) https://ir.aboutamazon.com/news-release/news-release-details/2021/Amazon.com-Announces-Third-Quarter-Results/

\(^{72}\) https://www.nbcnews.com/business/business-news/amazon-now-employs-almost-1-million-people-u-s-or-n1275539
Recently, Amazon’s CEO of World Consumer predicted that by early 2022, Amazon would surpass UPS and FedEx to become the U.S.’ largest package delivery service.76

Amazon has achieved this growth and dominance by creating a high-turnover, high-pressure system that offloads the costs of injuries, employment precarity, and deskilling onto the public, workers, and their families. This is Amazon’s great innovation. Monitored at every minute, Amazon warehouse workers and drivers report running to the bathroom or even peeing in bottles, suffering from mental stress and fatigue, workplace injuries, and being driven to unemployment. With turnover of 150%, or higher, Amazon itself worries that it will churn through the entire workforce in some regions.77

Amazon’s extensive worker surveillance and productivity metrics, commonly known as Rate and Time Off Task, have been repeatedly linked to the high injury rates at its warehouses.7879 In 2020, Amazon reported 27,178 workplace injuries, of which 90% were serious enough that workers were unable to perform their regular duties or were forced to miss work entirely.80 Studies have found that not only are serious injuries more frequent at Amazon warehouses—nearly 80% higher than for all other employers in the warehouse industry— but that they are more severe as well, with injured Amazon workers taking, on average, a week longer than the recovery time for workers injured in the general warehouse industry.8182 A study by Human Impact Partners also found that injury rates at Amazon warehouses were higher during the peak rush seasons associated with holidays, Cyber Monday, and Prime Day.83 Similarly, elevated injury rates were found at Amazon facilities with higher levels of robotic and automated technology.84

Amazon has also come to dominate the logistics industry by undercutting wages.85 A study by Bloomberg found that when Amazon opens new facilities, the average warehouse industry wages fall in that county, reaching their pre-Amazon level only after five years.86 The same study found Amazon’s employee promotion rate to be far below that of the industry average, reflecting the high turnover rate and lack of advancement opportunities facing most associates.87

Black workers disproportionately bear the brunt of Amazon’s model. At one of Amazon’s largest warehouses in New York, Black workers were fifty percent more likely to be fired than their white

---

73 https://www.cnbc.com/2021/06/18/as-e-commerce-sales-proliferate-amazon-holds-on-to-top-online-retail-spot.html
peers.\textsuperscript{88} And during the pandemic, Amazon fired several Black workers who spoke out about unsafe conditions.\textsuperscript{89} This mirrors findings that Black people are more likely to have dangerous jobs, less likely to have their concerns heard, and more likely to be retaliated against.\textsuperscript{90} Further, Amazon actively discourages the promotion of hourly workers in warehouses, the majority of whom are Black and brown.\textsuperscript{91}

Meanwhile, other employers are forced, lest they be undercut, to compete using the same methods that economist Daron Acemoglu calls “so-so” tech innovation\textsuperscript{92}. This so-so or low-road innovation contributes little to economic growth, while destabilizing the lives of working people and lowering wages. This race to the bottom wastes our enormous shared technological potential, while exacerbating economic inequality.

This is not a natural outcome of progress in the tech sector, but a reflection of economic policy decisions that we have the power to change. Our current policies incentivize the wrong kind of innovation and growth, and we must turn that around.

States are already beginning to take action in this direction. Recently, California passed a state bill regulating warehouse performance metrics such as those utilized by Amazon.\textsuperscript{93} In 2020, Washington state, citing the high workplace injury rates at Amazon warehouses, raised the company’s Worker Compensation premium rates by 15\% and proposed placing fulfillment centers in a risk class of their own.\textsuperscript{94} Worker surveillance practices like those Amazon uses to monitor associates and drivers, have also led to introduced legislation in Massachusetts and Illinois.\textsuperscript{95} \textsuperscript{96} Meanwhile, as Reuters reported last month, Amazon has used its massive lobbying and policy team to kill or undermine over 36 state bills that would impact the company.\textsuperscript{97}

As this committee studies actions to ensure we have a healthy tech sector, it should consider a new generation of economic policies and labor rights that prevent tech corporations like Amazon from leveraging worker exploitation into growth, and outcompeting rivals by taking the low road. Establishing robust worker protections and rebalancing power between workers and employers would not only benefit hundreds of thousands of Amazon workers, but could reorient the economy and tech innovation toward more equitable and sustainable outcomes that lead to productive growth. In order to do this, we must establish policies that prioritize worker health and safety, protect against predatory surveillance and automated management practices, fortify the rights of workers to speak out and organize, guard against low-road business models, and incentivize innovation that enhances worker well-being and shared economic prosperity.

\textsuperscript{88} https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html?referringSource=articleShare
\textsuperscript{89} https://sahanjournal.com/business-economy/amazon-shakopee-minnesota-protest/
\textsuperscript{90} https://www.nelp.org/publication/silenced-covid-19-workplace/
\textsuperscript{91} https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html
\textsuperscript{93} https://www.latimes.com/business/story/2021-09-08/california-bill-sb701-passes-senate-warehouse-work-metrics-algorithms-regulation
\textsuperscript{94} https://www.seattletimes.com/business/because-of-injury-claims-state-wants-amazons-automated-warehouses-to-pay-higher-workers-comp-premi ums-than-meatpacking-or-logging-operations/
\textsuperscript{95} https://www.bostonglobe.com/2021/10/07/opinion/massachusetts-has-chance-clean-up-our-national-privacy-disaster/
\textsuperscript{96} https://inthesetimes.com/article/at-will-just-cause-employment-union-labor-illinois
\textsuperscript{97} https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/
Dear Amazon Shareholder,

We are Amazon Associates and leaders with United for Respect (UFR) and the Warehouse Worker Resource Center (WWRC). We are part of a multiracial movement of working people advancing a vision of an economy where our work is respected and our humanity recognized. We write to you today to share an important letter from Human Impact Partners and over 200 public health practitioners calling on Amazon CEO, Andy Jassy, to end the inhumane and unsafe workplace quotas and surveillance that are currently ubiquitous throughout Amazon’s logistics network.

Based on the findings of a study by Human Impact Partners and the WWRC, this letter outlines the dangerous reality we experience going to work every day. The high productivity quotas at Amazon facilities, commonly known as rate and time off task, have led to injury rates twice that of the general warehouse industry, and three times that of the average private employer. During peak rush times, and in Amazon’s most automated facilities, workplace injury rates are even higher.

As the very people at-risk from Amazon’s unsafe warehouse practices, we urge you to read the letter and consider the included recommendations. Commonsense improvements such as doing away with rate and time off task, adopting ergonomic standards, and strengthening COVID-19 precautions would not only make Amazon facilities safer workplaces, but might lessen the worker shortage and high turnover rate seen presently at Amazon warehouses. As an Amazon shareholder, you can help mitigate any short-sighted mismanagement of human capital at the company and support any shareholder proposals that seek to review workplace health and safety issues.

In our capacity as Amazon, UFR, and WWRC worker-leaders, we would also welcome the chance to speak directly with you, answer any questions, and share our vision of a better and safer Amazon.

Sincerely,

United for Respect Member Leaders & the Membership of WWRC
Appendix IV: Joint Statement to Regulators and Lawmakers on Amazon Worker Surveillance (2021)

**Joint Statement**

**Stop Amazon’s Injury Crisis: End Amazon’s Dangerous and Punitive Worker Surveillance**

**June 21, 2021**

Amazon injures and discards warehouse workers and delivery drivers at double the industry average. There were a record 24,000 serious injuries at Amazon facilities last year. It is time for lawmakers and regulators to step-in and end the punitive system of constant surveillance that drives the dangerous pace of work at Amazon.

Amazon’s business model is a calculated exploitation of workers, the majority of whom are Black and brown. Amazon’s punishing system monitors workers’ speed or *rate*, tracks their movements each second with a metric called *time off task*, and imposes a constant threat of termination. Amazon claims to simply monitor workflow — but in reality, *rate* and *time off task* is used to control physical movements and discipline workers, dictate when or if they can use the bathroom, and has been used to retaliate against worker organizing. A recent investigation in Washington State concluded that this high-pressure system violates the law.

Discarding workers after they are injured or too exhausted, Amazon churned through over half a million workers in 2019. Amazon’s model breaks people’s bodies, taking their health and sometimes livelihoods. The cumulative costs of this exploitative business model are offloaded onto workers, their families, and the public.

Black workers disproportionately bear the brunt of Amazon’s model. At one of Amazon’s largest warehouses in New York, Black workers were fifty percent more likely to be fired than their white peers. And during the pandemic, Amazon fired several Black workers who spoke out about unsafe conditions. This mirrors findings that Black people are more likely to have dangerous jobs, less likely to have their concerns heard, and more likely to be retaliated against. Further, Amazon actively discourages the promotion of hourly workers in warehouses, the majority of whom are Black and brown.

Warehouse workers and delivery drivers cannot wait for Amazon to fix its broken system. To ensure Amazon’s model does not become the standard for our entire economy, regulators and lawmakers must intervene:

- **End rate and time off task tracking:** State and federal electeds should enact laws that ban this surveillance-driven discipline and control to ensure that workers are protected from abusive conditions.
- **Update OSHA standards and enforcement to end rate and time off task:** As evidence mounts that Amazon’s model creates an unsafe workplace, state and federal OSHA programs should enforce existing standards and create new rules that address practices like *rate* and *time off task* that monitor workers and increase the pace of work.
- **Investigate Amazon’s abuses:** Agencies tasked with safeguarding workers should investigate Amazon for these widespread and long-standing abuses, including: injuries, retaliation, and discrimination.

For years, workers have spoken out and protested against these conditions. Most recently, in Bessemer, Alabama, Black warehouse workers led a unionization effort, citing the punishing conditions created by Amazon’s system of surveillance, control, and threat of termination.

Last year, civil society organizations stood with workers and called upon Congress to ban this type of punitive worker surveillance, citing the dangerous impacts on workers’ physical and mental health, potential to undermine workers’ right to organize, and long-term deskilling and wage decline of these jobs.

Finally forced to admit to ongoing injury problems, Amazon is nevertheless doubling down on its extractive model. In his final letter to shareholders, Jeff Bezos stated that Amazon would begin to use artificial intelligence to direct workers from one task to the next. But using technology to maintain absolute control over workers’ tasks and workflow, it will only escalate Amazon’s injury crisis. Decades of research show that when workers do not have autonomy and control at work, they are more likely to be injured and experience mental strain and depression. Later, Amazon announced wellness programs and funding for injury research, but it refuses to do the one thing that would stop widespread injuries: eliminate rate and time off task.

Amazon will soon be the largest private employer in the United States, and if lawmakers and regulators fail to take action, its dangerous and extractive model will become the standard in warehousing, logistics, and retail. As other retailers implement similarly exploitative strategies, this dangerous trend will further degrade working conditions for tens of millions of people across the country. The result will be a punishing, untenable reality for all working people, and Black and brown people will pay the highest cost.

We call on lawmakers and regulators do everything in their power to end rate and time off task, ensuring Amazon cannot use this punitive system of surveillance to cycle through entire workforces in communities throughout the country.

In Solidarity,

Athena Coalition
Action Center on Race and the Economy (ACRE)
Awood Center
Al Now
Civil Liberties Defense Center
Color of Change
Constitutional Alliance
Demos
Fight for the Future

Free Press
Government Accountability Project
Green America
Institute for Local Self-Reliance
Jobs With Justice
LAANE
Make the Road New York
Make the Road NJ
MediaJustice
Movement Alliance Project
Appendix V: Joint Statement on Worker Surveillance (2020)

Joint Statement

Put Workers over Profits: End Worker Surveillance

Oct 14, 2020

Farhiyo Warsame, a warehouse worker, was targeted, surveilled, and fired by Amazon after speaking up about unsafe conditions at work, according to the Awood Center. Amazon tracked Farhiyo’s time in between each small task and used the accumulated extra seconds to justify threats for her eventual termination. Through this “rate” and “time off task” tracking system, Amazon would have you believe it monitors work productivity — but in reality, this system is used to control the physical movements of workers, dictate when or if they can use the bathroom, discipline workers and, in the end, has been used repeatedly to retaliate against workers. It enforces an unreasonable pace of work that leads to the unusually high number of injuries at Amazon.

Today, workers are subjected to an unprecedented level of workplace surveillance and control. From voice monitoring to tracking applications, these systems are being introduced into workplaces that are already stacked against low-wage workers, creating an environment ripe for exploitation. Surveillance gives corporations more power over workers. When combined with automation that dictates the pace and type of work, it results in a more dangerous, punishing, and precarious workplace. It can also lead to lower wages, deskilling of jobs, mental health stresses, the potential for racial discrimination, and a chilling effect on organizing. Workers urgently need legal protections that prevent these harms and end exploitative practices, including Amazon’s rate and time off task monitoring.

The use of surveillance to exploit workers has a long history in the United States, going back to the plantation and then in manufacturing, where Taylorism and other systems of “scientific management” established control over workers’ every move. The trend has worsened dramatically in recent years, and laws and regulatory agencies have failed to catch up.

Meanwhile, with few protections for workers, corporate employers have been able to grow profits by demanding and enforcing dangerous speeds, controlling each physical movement of a worker, and maximizing opportunities to make workers replaceable and expendable.
New technologies that monitor and control workers represent a radical transfer of power from workers to corporations. At Amazon warehouses, workers report that a scanner tells you exactly where to go, gives you seconds to get there, and then orders you what to do next. Your entire workload and every task you complete is managed in seconds. If you take longer than the seconds you are given, the time is added to your time off task. If you go to the bathroom or take a rest, this is also added to time off task. At the end of the day, if your productivity falls below a moving threshold, you are disciplined, and eventually fired.

Amazon’s contract delivery drivers face similar monitoring, with dispatchers pressuring drivers to deliver increasing volumes of packages in a single shift — even if that means drivers must speed or skip bathroom breaks to meet delivery quotas. At Amazon, this is paired with intelligence systems and practices to monitor potential organizing activity outside of work.

This level of monitoring and control has no place in our economy. Corporate employers say that these technologies make workplaces more efficient and are necessary to be competitive, but those claims do not hold up to scrutiny. Instead, we find:

**Individual productivity monitoring is used to enforce a dangerous pace of work.** Within Amazon warehouses, the pervasive and punitive nature of tracking rate and time off task for each worker results in nearly double the injury rate and greater job precarity, as compared to the sector. While Amazon claimed that they stopped disciplining workers for productivity during the pandemic, the practice continued. This type of monitoring is designed for workers to fail.

**Worker surveillance disproportionately harms Black and brown workers.** Black and brown workers are more likely to be in low-wage jobs, less likely to be listened to when they raise concerns, and more likely to face retaliation. Additionally, algorithmic decision-making can dramatically reinforce and exacerbate racial disparities, particularly where people impacted have no recourse or power. For many of these workers, the level of monitoring is akin to discriminatory police surveillance in their communities.

**Surveillance is being used punitively, rather than to keep workers safe.** Corporations are adopting new workplace technologies for the sole purpose of disciplining individual workers, even in areas where technology could be used to improve working conditions. When Amazon developed new technologies to determine if workers were within six feet of one another, they then immediately used this information to discipline and then fire workers.

**Surveillance is being used to retaliate against workers and undermine their protected rights to speak out and take collective action.** With limitless surveillance at an employer’s fingertips, targeting a particular worker is trivial — illegal retaliation is easily obscured. Amazon has used monitoring of time off task and social distancing to retaliate against workers after they spoke up about safety concerns. Surveillance of workers is not limited to the workplace, and it was recently reported that Amazon monitored private social media groups of Amazon Flex drivers, and tried to recruit an intelligence analyst to investigate labor organizing activities.

**Pervasive surveillance and automated control increase corporate profits on the backs of workers, by reducing wages and deskilling jobs.** While some technologies, such as supermarket scanners, allow companies to raise profits by using workers more efficiently, surveillance technologies raise profits by the cruder mechanism of increasing the exploitation of workers. The supermarket scanner allows each worker...
to serve more customers with the same level of effort, but surveillance technologies can dangerously accelerate the pace of work. The costs of injury and burnout are then offloaded onto families and the workers compensation system, rather than being internalized by the company.

During the pandemic, corporate employers have expanded workplace surveillance in ways that can compromise worker privacy and autonomy, and are using those tools for worker discipline and control. Employers have a legal duty to provide a safe working place (e.g. by slowing work speeds and providing handwashing breaks). Instead, Amazon developed a punitive social distance surveillance system that it gave to other corporate employers.

In response, state and federal governments should enact protections against workplace surveillance — ending predatory practices, such as Amazon’s rate and time off task monitoring. These protections should prioritize worker health and safety, fortify the rights of workers to speak out and organize, guard against low-road business models, require transparency in the use of new technologies, protect against new forms of tech-driven racial discrimination, and incentivize innovation that enhances worker well-being. Workers deserve better than models of exploitation developed on plantations and in factories over one hundred years ago.

In Solidarity,

Athena
Action Center on Race and the Economy
The Awod Center
Center on Privacy & Technology at Georgetown Law
Civil Liberties Defense Center
Color of Change
Constitutional Alliance
Council on American-Islamic Relations (CAIR)
Coworker.org
Demand Progress
Demos
Fight for the Future
Free Press
Government Accountability Project
Greater New York Labor-Religion Coalition
Instituto de Educacion Popular del Sur de California
Jobs With Justice
Just Futures Law
LAANE
Make the Road New York

Public Citizen
Restore The Fourth Minnesota
RootsAction.org
Secure Justice
SEIU California
Stand Up Nashville
SumOfUs
Surveillance Technology Oversight Project (S.T.O.P.)
United for Respect
Warehouse Worker Resource Center
Working Partnerships USA
X-Lab
Appendix VI: Joint Statement on Silencing Whistleblowers in the Workplace (2020)

Joint Statement

Silencing of Whistleblowers in the Workplace is a Threat to Public Health

May 5, 2020

Given the immediate public health risks, we are calling for an urgent expansion and improved enforcement of legal protections for workers who speak out and take collective action against dangerous workplace conditions that risk exacerbating the spread of COVID-19 in communities. Workers themselves are in the best position to raise health and safety concerns, and if these concerns are ignored, or worse, if workers are retaliated against, it not only impacts those workers and their families, but risks accelerating the current public health crisis.

Over the last few weeks, Amazon fired at least six workers who had spoken out about unsafe working conditions in warehouses. In addition to these firings, other workers at Amazon have reported receiving arbitrary work-related warnings as a result of speaking out or participating in walkouts, and they fear that they are being set-up for termination. Given that Amazon is the second largest private employer in the United States and is significantly expanding its workforce during the crisis, this apparent pattern of retaliation is alarming.

Thousands of warehouse, delivery, and grocery workers are on the front lines of this fight, risking contracting and spreading COVID-19 every day in order to provide essential goods. This risk disproportionately falls on communities of color, who are more likely to hold these jobs and more vulnerable to the virus, as a result of the systemic racism that undermines health in these communities. These essential workers are calling for common sense measures in line with CDC guidance: implementation of six feet of distance between all individuals in the facility, personal protective equipment for all, time for handwashing, temporarily closing and cleaning exposed facilities to allow for quarantine, independent and transparent reporting, and paid leave policies to help exposed and sick workers to stay home.

Instead of adopting policies to protect workers, corporations are increasingly adopting invasive surveillance technologies to penalize and monitor lower-wage workers. This already predatory surveillance could too easily be turned against protected concerted activity and workers voicing concerns. We know that the mere presence of pervasive surveillance is likely to silence dissent, but not to protect health.

People who take action and speak out are not only exercising their legally protected right to protest and organize collectively for safe working conditions, but also acting in the national interest and protecting public health. Large facilities like warehouses, factories, and meatpacking plants employ thousands of people and grocery stores are major points of social interaction — if necessary precautions are not taken, COVID-19 could easily spread throughout communities. The right to demand better health and safety measures needs to be protected in order to limit the spread of COVID-19.
The current crisis has elevated workplace whistleblowing and collective action to a matter of national health and additional protection and enforcement measures are urgently necessary.

In Solidarity,

Athena Coalition
Access Now
Action Center on Race and the Economy
AI Now Institute
Alternate ROOTS
Black Alliance for Just Immigration
Center on Privacy & Technology at Georgetown Law
Color of Change
Community Justice Exchange
Constitutional Alliance
Council on American-Islamic Relations (CAIR)
Defending Rights & Dissent
Demand Progress Education Fund
Ella Baker Center
Fight for the Future
Freedom of the Press Foundation
Global Action Project
Government Accountability Project
Instituto de Educacion Popular del Sur de California
Just Futures Law
Line Break Media
Make the Road New Jersey
Make the Road New York
Media Mobilizing Project
MediaJustice
MPower Change
Muslim Advocates
National Employment Law Project (NELP)
National Immigration Law Center
New America Center on Education and Labor
New America’s Open Technology Institute
New York Communities for Change
Ohio Valley Environmental Coalition
Open Markets Institute
Open MIC (Open Media and Information Companies Initiative)
Partnership for Working Families
People Demanding Action
People For the American Way
PeoplesHub
Project Censored
Project On Government Oversight
Public Citizen
RootsAction.org
RYSE Center
Secure Justice
Surveillance Technology Oversight Project (STOP)
The Awood Center
The Civil Liberties Defense Center
The Tully Center for Free Speech
United for Respect
United We Dream
Warehouse Worker Resource Center
Whistleblower & Source Protection Program at ExposeFacts
Woodhull Freedom Foundation
XLab
Appendix VII: Memo to the White House Task Force on Worker Voice (2021)

MEMO
Subject: Key Issues and Recommendations on Worker Surveillance & Algorithmic Management
From: The Athena Coalition
Date: December 2021


Introduction

Surveillance technologies and algorithmic management systems in the workplace operate hand-in-hand to facilitate corporate subversion of workers’ legal rights while eroding the little power that workers have to improve their own working conditions. Across many sectors, programs such as biometric monitoring, social media surveillance, GPS location tracking, and automated termination are radically reshaping jobs and the relationship between workers, their managers, and employers. Workers have few meaningful protections or rights related to these technologies, and as a result there are real material costs to their job quality, compensation, job stability, and physical and mental health. Left unchecked, companies using such technologies to increase their bottom line will continue to propel the nation’s workforce towards a bleak, hostile, and dehumanized future.

Key Issues & Harms to Workers

1. **Worker Health & Safety:** The combination of continuous digital surveillance, automated task management, punitive productivity quotas, aggressive “time off task” (TOT) tracking, and strict termination measures results in dangerous and unhealthy working conditions; frequent and serious worker injuries; extreme turnover rates; and psychological damage such as anxiety, depression, and suicidality.

2. **Interference with Right to Speak Out and Organize:** Surveillance of workers’ activities, movements, locations, communications, and social media accounts—including predictive heat maps and detailed tracking software—violate workers’ legally protected rights to unionize and organize, and their rights to free expression and assembly, by pre-empting or disrupting unionization efforts and other forms of collective action and giving employers small excuses to disguise retaliation against organizers and whistleblowers.

3. **Racial Injustice & Civil Rights:** Worker surveillance and worker rights violations are a racial justice and civil rights issue. Black workers disproportionately bear the brunt of Amazon’s model, with one New York warehouse being nearly 50% more likely to fire them; Black whistleblowers are over 200% more likely to face retaliation; Amazon has predominantly targeted and neglected Black employees; and many companies that implement invasive worker surveillance and algorithmic management programs predominantly employ Black, Brown and other workers of color. All of this occurs in conjunction with algorithmic racism; discriminatory police surveillance and technological bias against Black and other racialized communities; a history of anti-Black surveillance rooted in slavery; and data-driven discrimination and pre-existing workplace inequity based on race, gender, disability, sexual orientation, and other protected characteristics.

4. **Information Asymmetry:** US employment and labor law grants employers all but unilateral power over their premises and technologies, the details of which are often withheld from the very workers subjected to them. This results in severe information asymmetry and an even greater power imbalance between workers and employers, with companies knowing more about workers than they know about themselves, whether they know
it or consented or not, and workers having no equivalent window into employers’ activities against their interests. Lack of corporate transparency also contributes to information asymmetry with regulators and the public, such as Amazon concealing the extent of its worker injury crisis.

5. **Race to the Bottom:** Amazon’s market size in shipping and retail, combined with the extremity of its unethical worker surveillance and automated management practices, further push competitors’ practices and related industry standards to deteriorate even for unionized workers, in an ever-intensifying race to the bottom for workers who are the most vulnerable to surveillance-fuelled abuse. Widespread adoption of Amazon’s model also represents the private sector offloading its traditional responsibilities onto workers themselves and the public, with government funds subsidizing corporate exploitation through social welfare and health care programs shouldering the consequences of inhumane and injurious workplaces.

**Potential Legal Violations**

Extensive documentation such as media reports, published research, and workers’ testimonies provide evidence to suggest that Amazon’s apparatus of worker surveillance and algorithmic management, and that of other companies engaging in similar practices, amount to violations of numerous labor and employment laws. The following list provides high-level examples using key relevant statutes, and is by no means exhaustive:

1. **Title VII of Civil Rights Act:** Amazon’s practices may provide grounds for several Title VII violations, such as penalizing workers based on disability or religion, or selectively disciplining Black or other racialized workers for minor infractions which may be overlooked if committed by white peers or workers who do not raise health complaints or promote unionization. Amazon has also reportedly engaged in pregnancy discrimination, which is especially concerning in light of employers’ access to employees’ fertility and menstrual tracking app data.

2. **Americans with Disabilities Act (ADA):** Amazon’s intentionally labyrinthine leave and accommodations system and their punitive time-off-task and rate measures, which all but prohibits breaks, likely violates the ADA’s requirement of reasonable accommodations for workers with disabilities. Workers have sued Amazon for failing to accommodate conditions such as Crohn’s disease, irritable bowel syndrome, and cardiovascular medical issues. Further analysis applying the ADA to worker surveillance and automated management is available here.

3. **Occupational Safety and Health Act (OSH Act):** According to an OSHA interpretation letter cited in this report, OSH Act standards require that “employees are able to use toilet facilities promptly” and “[r]estrictions on access must be reasonable, and may not cause extended delays.” Given copious documentation that workers severely delay relieving themselves or are not able to use provided facilities at all, as a direct consequence of surveillance-enabled rate and time-off-task measures, Amazon appears to violate this Act. Amazon may also violate OSH Act’s anti-retaliation provisions given its response to COVID-19 whistleblowers.

4. **Fair Labor Standards Act (FLSA):** Amazon places surveillance-enabled and productivity quota-driven demands on the delivery drivers it contracts with as much as on its employees; such drivers are likely misclassified Amazon employees, given the level of granular control the company exerts over them. Amazon’s punitive monitoring and corresponding pressure has resulted in multiple lawsuits from delivery drivers for wage theft and failure to provide required rest and meal breaks under the FLSA.

5. **National Labor Relations Act (NLRA):** The NLRA prohibits employers from either surveilling or creating an “impression of surveillance” of unionization activity, as an unfair labor practice. Evidence indicates that Amazon deliberately engages in anti-union surveillance activities, in violation of these requirements.
Recommendations

1. **Joint Task Force**: Establish an inter-agency joint task force dedicated to worker surveillance and algorithmic management of low-wage workers across key industries such as logistics and retail.

2. **Inter-Agency Systemic Investigation**: Launch an inter-agency investigation into the widespread and longstanding patterns of abusive and unethical practices at Amazon, addressing them as systemic, company-wide issues rather than one-off cases tied to specific individuals. Such issues include high worker injury rates, occupational safety and health, persistent retaliation issues, discrimination based on protected characteristics such as race or disability, and interfering with collective organizing activities.

3. **Discrimination and Disparate Impact Investigation**: Investigate worker surveillance, algorithmic management, and use of biased technologies such as facial recognition at Amazon, for discriminatory treatment or disparate impact on Black, Brown, and other racialized workers, as well as on historically marginalized workers based on gender, disability, or other characteristics protected in human rights and equal employment opportunity law.

4. **End Punitive Uses of Worker Surveillance**: Restrict companies from using worker surveillance towards punitive ends, such as interfering with unionization efforts and related forms of collective organizing, or relying on worker data generated through electronic monitoring alone for disciplinary measures and termination.

5. **End Rate & Time-Off-Task Policies**: Update or promulgate new OSHA standards and strengthen enforcement to end rate and time-off-task policies, as well as invasive surveillance used to intensify work, to address their damaging physical and mental health and safety consequences.

Sources and Further Reading

*Data and Algorithms at Work: The Case for Worker Technology Rights* (UC Berkeley Labor Center); *Little Tech is Coming for Workers* (Coworker.org); *The Public Health Crisis Hidden in Amazon Warehouses* (Human Impact Partners and Warehouse Worker Resource Center); *Amazon's Disposable Workers: High Injury and Turnover Rates at Fulfillment Centers in California* (National Employment Law Project); *The Constant Boss: Labor Under Digital Surveillance* (Data & Society); *Eyes Everywhere: Amazon’s Surveillance Infrastructure and Revitalizing Worker Power* (Open Markets Institute); *Warning: Bossware May Be Hazardous to Your Health* (Center for Democracy & Technology); *Athena Joint Statements; Color of Surveillance 2019: Monitoring of Poor and Working People: Reading List* (Center on Privacy & Technology at Georgetown Law).
The National Women’s Law Center submits the attached comment in response to the Request for Information by the White House Office of Science and Technology Policy regarding the impact of automated surveillance and management in the workplace on workers' rights, opportunities, health, and safety. We appreciate the opportunity to provide comments on the impact of automated surveillance and management on women workers, particularly women of color and low-paid women workers. Please see attached comment.

Attachments

NWLC Comment - OSTP RFI Electronic Surveillance and Automated Management Systems
OSTP_FRDOC_0001-0008 6-29-2023
June 29, 2023

White House, Office of Science and Technology Policy
Executive Office of the President
Attn: Alan Mislove, Assistant Director for Data and Democracy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Submitted via regulations.gov

Re: Comments on Automated Worker Surveillance and Management,
OSTP_FRDOC_0001-0008

Dear Mr. Mislove:

The National Women’s Law Center (NWLC) submits this letter in response to the Request for Information (RFI) by the White House Office of Science and Technology Policy (OSTP) regarding the impact of automated surveillance and management in the workplace on workers’ rights, opportunities, health, and safety.¹ The National Women’s Law Center has worked for over 50 years to advance and protect women’s equality and opportunity—with a focus on women’s employment, education, income security, health, and reproductive rights—and has long worked to remove barriers to equal treatment of women in the workplace. We applaud OSTP for recognizing the increasing prevalence of automated surveillance and management in the workplace and its potential to cause myriad harms to workers.

We write specifically to raise the ways in which working women, especially women of color and low-paid women, may be negatively impacted by the use of electronic surveillance and automated management (ESAM) systems in the workplace that threaten to exacerbate discrimination, lead to violations of employment and labor laws, and reduce job quality—and quality of life—for workers. ESAM tools may have outsized negative effects on women, people of color, and low-paid workers because of structural inequities in the workforce and society. Women, people of color, and low-paid workers tend to be disproportionately represented in industries in which potentially problematic use of ESAM may be likely, such as caregiving,

hospitality, warehouses and call centers. Moreover, women—especially Black, Latina, and Native women, women with disabilities, and immigrant women—and LGBTQI+ individuals have also long been disproportionately likely to experience poverty and hardship. Workers living from paycheck to paycheck may feel constrained seeking to enforce workplace protections given the very real fears of retaliation. And many women and people of color lack union representation and/or work in the industries where corporate misclassification is rampant, further compounding the potentially harmful impacts of ESAM. Given these considerations, OSTP should ensure that employers relying on ESAM understand the impact of these systems on their workforce as well as their continuing legal obligations under anti-discrimination and employment law.

We offer a series of recommendations for the Administration to consider as it works to prevent and address these impacts, especially as a growing number of companies are using ESAM to hire and monitor their workforce.

I. ESAM and Discrimination in the Workplace

As discussed above, women, people of color, and low-paid workers may be particularly susceptible to potential harm from ESAM. ESAM tools may exacerbate existing patterns of discrimination and increase the risk of additional discrimination. On top of these challenges,


3 Jasmine Tucker, Sarah Hassmer, Amy Matsui, Melissa Boteach, and Cara Claflin, BY THE NUMBERS: Data on Key Programs for the Well-Being of Women & Their Families, National Women’s Law Center (June 2021).


5 While there are no comprehensive, validated data indicating precisely how many companies are using these technologies – and companies are generally not required to report or disclose their use – one study estimated that 60% of large employers were using tools to track their workers, with the number expected to rise. Jordan Turner, The Right Way to Monitor Your Employee Productivity, Gartner (June 9, 2022), https://www.gartner.com/en/articles/the-right-way-to-monitor-your-employee-productivity.

6 In the hiring context, we have already seen how AI algorithms can replicate bias and discrimination, including by relying on proxies for protected classes to make employment-related decisions. Jeffrey Dastin, Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women, REUTERS (Oct. 9, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruitingtool-that-showed-bias-against-women-idUSKCN1MK08G.
ESAM often lacks transparency, with workers not knowing what data is being collected and how it is being used, creating a very real possibility that any incorporated biases and discriminatory impacts will be difficult to identify, review, or challenge.

Below we identify several ways in which ESAM may create a potential for discrimination for protected groups.

**Productivity standards**

One common use of ESAM is to impose production quotas, which are designed to maximize productivity and may result in an increased pace of work, discouraging and even penalizing workers from taking breaks or downtime. Because of the often relentless pace of productivity standards, they may operate in a way that fails to accommodate protected workers.

One group of protected workers who may face potential discrimination in the face of ESAM’s productivity standards are pregnant and lactating workers, some of who may need more frequent breaks, rest time, or other reasonable accommodations than may be permitted under the productivity standard. Without ensuring a design and application that can accommodate protected groups, ESAM imposed productivity standards could exacerbate discrimination and result in workplace discipline, termination, and other harms. Amazon, for example, has faced lawsuits from multiple pregnant women alleging discrimination and is notorious for its “proprietary productivity metric.” The Pregnant Workers Fairness Act and the PUMP for Nursing Mothers Act, which is built on the Break Time for Nursing Mothers Act, provide new protections for these workers, but it may be challenging for workers to enforce their rights to these protections given the opaque nature of ESAM’s productivity standards, the lack of information shared with workers, and the concerns many workers may have regarding retaliation.

Low-paid pregnant workers of color are likely to be especially vulnerable to harm in the face of ESAM’s productivity standards. Over one in five pregnant workers are employed in low-paid jobs, which are particularly likely to be physically demanding. Moreover, pregnant Black women and Latinas are disproportionately represented in low-paid jobs and especially likely to stand, walk or run continuously during work, and may be more likely to need an accommodation

---


8 See Alfred Ng & Ben Fox Rubin, *Amazon Fired These 7 Pregnant Workers. Then Came the Lawsuits*, CNET (May 6, 2019), [https://www.cnet.com/tech/tech-industry/features/amazon-fired-these-7-pregnant-workers-then-came-the-lawsuits/](https://www.cnet.com/tech/tech-industry/features/amazon-fired-these-7-pregnant-workers-then-came-the-lawsuits/).


11 Id.

12 Morgan Harwood and Sarah David Heydemann, *By The Numbers: Where do Pregnant Women Work?*, National Women’s Law Center (June 2021), [Pregnant-Workers-by-the-Numbers-v3-1.pdf](https://nwlc.org/). Over one in five pregnant workers are employed in low-wage jobs, which are particularly likely to be physically demanding.
at some point during pregnancy to continue to work safely.\footnote{Id. Lack of access to these important protections can result in significant harm to protected groups of workers, such as increased vulnerability of low-paid pregnant workers to health effects of physically demanding work, including preterm birth, low birth weight, miscarriage, and stillbirth.}

**Data Collection**

The increased ability of ESAM to gather more extensive and personal data about workers—often without informed consent—could open the doors to increased discrimination in the workplace.\footnote{See Zickuhr, supra note 2.} ESAM facilitates employers’ access to sensitive personal information, including health data, religious practices, family structure, race, gender, sexuality, and nationality/immigration status. For example, data collection on health can capture information about fertility, pregnancy, abortions, gender affirmation procedures or other private health data. It is not an unfounded fear that these tools may become additional opportunities for employers to discriminate in the workplace. Pregnant workers already face significant discrimination.\footnote{Giftis, Sprick, and Schweer, \textit{BPC – Morning Consult: 1 in 5 Moms Experience Pregnancy Discrimination in the Workplace}, Results from National Tracking Poll, Bipartisan Policy Center (Feb. 4-6, 2022), BPC – Morning Consult: 1 in 5 Moms Experience Pregnancy Discrimination in the Workplace | Bipartisan Policy Center.} Given widespread state-level restrictions on abortion access, and the proliferation of state laws targeting LGBTQI+ individuals, the misuse of ESAM by employers, or of the data collected by these tools, could lead to severe consequences for workers seeking to become pregnant, access abortions or obtain gender affirming care.

One example of such invasive and potentially discriminatory tools are workplace wellness apps, which could provide employers with data that leads to discrimination. While workplace wellness apps have been in use for years, the increasing development and prevalence of ESAM enable employers to gather even more potentially harmful data on their workers.\footnote{Bernhardt, Kresge and Suleiman, supra note 2, at 4.} For example, a recent pregnancy-tracking app gathered information about menstruation, fertility and pregnancy, and, in at least one instance, the health data (in a “de-identified,” aggregated form) was shared with employers.\footnote{Drew Harwell, \textit{Is your pregnancy app sharing your intimate data with your boss?}, The Washington Post (Apr. 10, 2019). \url{https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?arc404=true}. The pregnancy-tracking app Ovia lets women record their most sensitive data for themselves — and their boss.} Even in its “de-identified” form, the information shared with employers could provide individually identifiable findings if the workplace has few women of child-bearing age or few pregnant women, or if employers are able to piece together information from the broader sets of data they collect. It is concerning that employers are able to access and track such personal and private data, as it could lead to increased adverse employment actions against workers. For example, an employer could terminate or fail to promote an individual based on pregnancy before a worker even disclosed their status to their employer. With the opaque nature of ESAM and data collection, it could be extremely challenging for a worker facing such discrimination to recognize it or prove it.
Emotion Recognition

Another troubling category of ESAM consists of so-called “emotion recognition” technologies, which can exacerbate discrimination in the workplace.18 Research indicates that these systems are both less accurate19 and more likely to assign negative emotional states when analyzing women and people of color.20 Such tools also may internalize and repeat existing discriminatory stereotypes about how women “should” act or speak and may represent an automated form of the “tone policing” that occurs with women of color, and Black women in particular. Thus, these systems are likely to have outsized negative effects on women, people of color, LGBTQI+ persons, disabled workers, and other historically underrepresented and marginalized groups and could lead to discrimination based on gender, race, disability and national origin. When used as a tool to measure performance, for example, inaccurate assessments for protected workers could result in discriminatory employment decisions and actions, such as lack of access to bonuses, discipline of or failure to promote affected workers, as well as increased burdens to comply with work requirements. As an example, call centers, where women represent the majority of workers,21 may use emotion recognition to monitor their workforce, resulting in confusing, misleading and harmful negative feedback.22 In response to such monitoring, Communications Workers of America has negotiated protections for call-center workers with respect to monitoring technology.23

Online Reviews

ESAM can also lead to discrimination when platform companies rely on online reviews to evaluate, promote and even remove workers from their platforms.24 Multiple studies have found evidence of racial and gender bias in online reviews, with users giving lower and/or fewer ratings to Black workers and women than to white workers and men.25 The growth of online platforms and their continued reliance on online reviews both to make workplace decisions and as part of workers’ profiles could exacerbate workplace discrimination. Of particular concern is the failure of such platforms to ensure a mechanism to correct for customer gender and racial bias.26

22 Yang, supra note 7, at 235-236.
24 See, e.g., id.
25 Id.
26 See, e.g., Kati Sipp, Ratings in the Gig Economy Are a Mess. Here’s How to Fix Them, Wired (Dec. 27, 2017), The Gig Economy’s Rating System Is a Mess. Here’s How to Fix It. | WIRED. There is a line of Title VII cases finding that customer bias is not a permissible rationale for employer bias. See, e.g., EEOC v. Treatment Centers, LLC d/b/a
Sexual Harassment, Assault and Stalking

Another significant challenge for women, LGBTQI+ people, and workers of color is workplace harassment and assault. ESAM presents both risks and opportunities for workers with respect to this potential workplace discrimination. For example, ongoing surveillance could help ensure that workers seeking assistance to address harassment or assault could receive rapid, responsive help or could help employers find and respond to patterns of discrimination. However, ESAM also could create dangerous opportunities for harassment and stalking in the workplace unless there are intentional efforts to prevent such abuses. In the wrong hands, for example, ESAM could enable an abuser or harasser to track a victim’s every move, greatly increasing workplace stalking, which includes “[m]onitoring and/or surveilling the victim while at work; [t]racking software on work devices, [m]onitoring workplace communications for information about the victim.”27 Millions of people are stalked every year in the United States—of the roughly 42% stalking victims who are stalked by an acquaintance, about one-fourth of those are professional acquaintances.28 The negative impacts of work-related stalking are far-reaching; they include diminished performance, work disruptions, violence at the workplace, and losing both one’s job and sense of safety altogether.29

II. ESAM and Job Quality

As discussed above, women and people of color are disproportionately represented in industries that may utilize ESAM, and many of these jobs are considered precarious work—including part-time, temporary, and contract work.30 Low-paid, part-time, and contract workers are less likely than workers in traditional, full-time employment to have jobs with stable schedules, predictable incomes, or benefits. Unfortunately, ESAM is being used in ways that can magnify these problems and create other job quality challenges, such as invasive surveillance. Below are a few examples of how ESAM can harm work quality for many women and workers of color.

---

27 “Stalking is a pattern of behavior directed at a specific person that would cause a reasonable person to feel fear or suffer emotional distress.” Stalking Prevention, Awareness, and Resource Center, Workplaces Respond to Domestic & Sexual Violence, and FUTURES Without Violence, Stalking and the Workplace: Fact Sheet (Jan. 2023).

28 Workplace Stalking Fact Sheet (stalkingawareness.org).


Scheduling
Employers have increasingly used ESAM to set worker schedules in ways that can negatively impact worker autonomy and quality of life. ESAM causes significant disruption in workers’ ability to anticipate their workweeks and plan accordingly because the use of scheduling algorithms often produces erratic schedules. Workforce management systems use algorithms to base workers’ schedules on perceived consumer demand and maximize flexibility for the employer at the expense of the employee. Unpredictable scheduling can be especially detrimental for women, who are often concentrated in the service sector jobs in which unpredictable hours are prevalent and still shoulder the majority of caregiving responsibilities in families. Women of color are especially likely to be breadwinners for their families, and also are more likely to experience scheduling instability than their white counterparts. For mothers responsible for child care and checkups, for pregnant workers needing to attend multiple medical appointments, and for the many other responsibilities of life, control over scheduling is key to the ability to successfully manage work, personal and family responsibilities. Predictability regarding earnings is also important to be able to budget for rent, food, child care and other child-related expenses, such as diapers. In addition, erratic work schedules can make it nearly impossible for workers to pursue further education or training while holding down a job. A worker’s inability to access workforce training programs or education in turn makes it more difficult for them to move into higher-paying jobs, negatively impacting longer-term economic security.

Productivity Standards
As discussed above, ESAM is often used to impose productivity standards, many times at unsustainable levels. In addition to the potential discriminatory impact already discussed, productivity standards may also lead to significant reductions in work quality and quality of life for many workers. The pace of work resulting from ESAM’s productivity standards often results in musculoskeletal strain, an increased likelihood of accidents and workplace injuries, as well as mental health consequences. The risk of physical injury arises from the increased pace of work, a decrease in breaks and other forms of downtime that protect workers’ bodies from physical strain, and the physical manifestations of the mental health effects of ESAM. Such harm includes the physical injuries that are the natural result of a punishing and often repetitive pace of work, as well as the inability to follow safety practices due to time constraints.

31 See, e.g., Zickuhr, supra note 2, at 17.
33 See, e.g., Samantha Fields, Child care is a challenge for the many parents with unpredictable work hours, Marketplace (June 12, 2023), https://www.marketplace.org/2023/06/12/unpredictable-work-schedules-for-parents-make-child-care-a-huge-challenge/.
35 Scherer, supra note 34.
relentless pace of work and lack of downtime also lead to mental strain, depression and anxiety.\textsuperscript{36} Because women and people of color are more likely to be working at worksites using such ESAM, they are also more likely to experience these risks to their health and safety.

**Surveillance of Caregivers**

ESAM raises multiple privacy concerns that reduce the quality of work for paid caregivers, compounding the precarious working arrangements many already face.\textsuperscript{37} In-home caregivers, the majority of whom are women, and disproportionately women of color or immigrants, \textsuperscript{38} are often uniquely exposed to surveillance and public exposure. Many nannies, for example, work in homes with “nanny cams” that can record both their images and their voices.\textsuperscript{39} In addition, new apps such as “stroller patrol” encourage bystanders to capture and post images of nannies engaged in perceived wrongdoing.\textsuperscript{40} Such images can be shared widely, resulting in public shaming and reputational harm for nannies, who have limited opportunity to respond.\textsuperscript{41} The increasing use of online marketplaces to seek employment further exposes nannies to public scrutiny, as they often feel pressured to share personal details, such as family status and photos, in order to improve their chances of employment.\textsuperscript{42} Workers’ profiles also show ratings based on customer reviews and other metrics, and can influence workers’ chances of being hired. As discussed above, customer ratings may reflect societal discrimination against people of color, yet the systems do not provide a way to correct for these biases. Care workers have also noted that while employers are able to review workers, there is no opportunity for workers to provide feedback on employers, including to flag sexual harassment, wage theft or other workplace violations.\textsuperscript{43}

Another example of potentially invasive and harmful ESAM affecting paid caregivers is electronic visit verification (EVV), a recent Medicaid requirement that requires personal care and home health services workers to electronically verify information regarding their home visits.\textsuperscript{44} The EVV systems vary from state to state, with some systems that are overly invasive and

---

\textsuperscript{36} Id.; Nguyen, supra note 2.

\textsuperscript{37} Zickuhr, supra note 2, at 14.


\textsuperscript{43} See, e.g., Bernhardt, Kresge and Suleiman, supra note 2, at 8; Ticona, Mateescu, and Rosenblat, id. at 28.

complicated, tracking workers’ locations, attendance, and work duties, and often requiring workers to use handheld devices, wearables, or even biometric recognition systems.\textsuperscript{45} Both patients and workers suffer from EVV workplace mandates that force caregiving into timed physical tasks with limited autonomy over caregiving that fail to allow for flexibility for individual circumstances.\textsuperscript{46} On top of the autonomy and privacy implications, some of the EVV systems require workers to manage a demanding technology—time for which they may not be paid.\textsuperscript{47} In Arkansas, for example, home care workers faced lost or delayed wages in addition to increased surveillance as a result of EVV.\textsuperscript{48} Again, the burden of this surveillance is born disproportionately by women, as the majority of paid home care workers are women, and often women of color or immigrants.\textsuperscript{49}

### III. ESAM and Employment and Labor Protections

Structural inequalities in the workplace exacerbate vulnerability to harm from ESAM, impacting workers access to union representation, increasing worker misclassification, and negatively impacting wages and working conditions. Workers may also face greater challenges enforcing their protections in the face of ESAM.

**Barriers to Unionization**

The potential impacts of ESAM on women’s wages, working conditions and benefits are compounded in non-union workplaces where some companies are using ESAM to identify and disrupt workers’ efforts to organize themselves and push back against harmful workplace practices.\textsuperscript{50} Amazon, for example, has sought to hire analysts and purchase software that would allow it to monitor “labor organizing threats” and analyze data on unions.\textsuperscript{51} Given that very few women in the workforce are union members—just 9.6% in 2022\textsuperscript{52}—ESAM threatens to further impede women’s ability to improve their wages and other benefits through union membership. Union membership has clear advantages for women workers, and particularly for Black and Latina women.\textsuperscript{53} For example, women who are union members typically make $205 more per

\textsuperscript{45} Bernhardt, Kresge and Suleiman, supra note 2, at 8; Brown, supra note 38.

\textsuperscript{46} See, e.g., Mateescu, supra note 44.

\textsuperscript{47} Virginia Eubanks and Alexandra Mateescu, ‘We don’t deserve this’: new app places US caregivers under digital surveillance, The Guardian (July 28, 2021).

\textsuperscript{48} Id.

\textsuperscript{49} Brown, supra note 38.


\textsuperscript{51} Palmer, id.


week than women who are not union members;\(^54\) and while the gender wage gap persists even when women are unionized, women in unions are consistently paid wages that are not just higher but also more equal to men’s wages.\(^55\) Moreover, union members are more likely than non-union members to have access to other benefits, such as health benefits and paid sick days.\(^56\) And, of course, union membership enables members to enforce their rights through a grievance procedure, making it more likely that unionized workers will feel comfortable enforcing their rights in the face of ESAM-related legal violations or other harms.

**Misclassification of Workers**

The intersection of ESAM and corporate misclassification further exacerbate the harms associated with each, and disproportionately impacts women and people of color, as they are overrepresented in the low-paid, labor-intensive industries in which misclassification is common, such as delivery services, janitorial services, transportation, and home care, as well as in app-dispatched work.\(^57\) ESAM enables employers to closely control workers—for example, unilaterally setting fee rates, dictating when and how workers interact with customers—while imposing take-it-or-leave-it independent contractor agreements on their workforce.\(^58\) Digital labor platform companies are emerging in sectors like retail\(^59\) and food service,\(^60\) in which the majority of the workforce historically has been engaged as payroll employees. In digital labor platform work, Black and Latinx workers are overrepresented by 45 percent—more than in traditional misclassification prone sectors.\(^61\) All workers who are misclassified suffer from a lack of workplace protections, but women, people of color, and immigrants face unique barriers to economic security and disproportionately must accept low-paid, unsafe, and insecure working conditions.

---


\(^{56}\) Fins, Heydemann, and Tucker, supra note 53.


Compensation for gig platform workers, which is often opaque and confusing, illustrates how ESAM can exacerbate barriers facing gig workers. A 2021 report by the Pew Research Center found that fewer than half of gig workers understood how the companies for which they work determine how much they get paid.62 Some gig platform companies use ESAM in ways that increase this information asymmetry and result in lower and inconsistent earnings for workers, including gender pay gaps.63 Companies may use data mining and ESAM to estimate and pay the lowest amount that the worker will accept to engage in desired behaviors.64 Given the longstanding wage gap for women’s pay, it is not hard to imagine that such a system could result in lower pay for women than men. Some gig-economy platforms exploit this ambiguity by combining low overall pay with volume and time-based incentives that maximize workers’ time on the platform while minimizing workers’ take-home pay.65

**Lost compensation**

ESAM also has resulted in loss of earned compensation for some workers. ESAM tools that integrate timekeeping and payroll systems give employers the ability to automatically dock workers’ pay for time spent away from the computer or time off task.66 Protected workers who may need more frequent breaks, such as some women who are pregnant or breastfeeding, could be disproportionately impacted by such ESAM-driven practices.

**Enforcement of workplace rights**

Intrinsic in the analysis of the impact of ESAM on workers’ rights is the ability of workers to exercise and enforce their workplace rights. As discussed above, ESAM may be used by some employers to push workers to meet productivity standards that may limit their access to legally required breaks or accommodations, to monitor workers for potential “labor organizing threats,” to dock workers’ pay, to misclassify workers, and more.67 The lack of transparency regarding ESAM in the workplace, the intimidation of workers through ongoing surveillance, and the increased challenges workers face discussing workplace protections and collective action without detection create multiple barriers to the ability of workers both to identify violations of their workplace rights and to enforce their rights.

---


63 See generally Veena Dubal, *On Algorithmic Wage Discrimination* (Jan. 19, 2023), [https://ssrn.com/abstract_id=4331080](https://ssrn.com/abstract_id=4331080) (citing a 2020 study showing that women working for Uber make roughly seven percent less than men and pointing to “the structure of the wage setting—by algorithmic wage discrimination” as the basis for pay differences despite Uber research explanation that the wage differential resulted from worker experience, driver speed and “rideshare specific human capital”).

64 See generally id.


67 Zickuhr, supra note 2.
IV. Recommendations

Research
The administration must conduct research and commission studies to better understand and address the impacts of ESAM on workers, with a focus on the rights and experiences of protected groups. Research must encompass how ESAM and ESAM-driven practices may facilitate or obfuscate workplace discrimination, and otherwise impact earnings, workplace discipline and promotions, working conditions, workplace injuries and fatalities, scheduling, and physical and mental health. Research should also examine the impact of ESAM on workers’ ability to associate and engage in collective bargaining as well as on the experience of gig workers and independent contractors. Finally, research should identify ways in which ESAM can protect workers’ rights, such as by using ESAM to detect or prevent workplace discrimination and harassment. Research should include findings disaggregated by demographic characteristics, including income, sex, gender identity, race and other protected categories.

Guidance and rulemaking
The administration must make clear the existing applicability of civil rights laws and other worker protections under ESAM. The Equal Employment Opportunity Commission (EEOC), Department of Labor (DOL) and the National Labor Relations Board (NLRB) should issue guidance, as well as regulations, under each of the statutes within their purview clarifying and detailing employers’ obligations to ensure that ESAM does not violate these laws, including the right to reasonable accommodation where applicable, and prohibiting uses of ESAM that harm or marginalize protected workers. The agencies must also conduct worker outreach to ensure that workers subject to ESAM are aware of their rights. Clarifying the mandate regarding legal applicability of and authority with respect to ESAM could help curtail many harmful applications of ESAM, although additional legislation is needed.

DOL and NLRB must also finalize rulemaking on joint-employer status. The rules must make clear that the use of ESAM to monitor and manage workers is evidence of control and weighs in favor of a finding of employer status.

As the Administration moves forward to research and regulate the impact of ESAM on workers, the principles within the Blueprint for an AI Bill of Rights should provide the administration with a framework to address ESAM practices that disadvantage protected worker groups.

Legislation
The Administration should engage with Congress to develop and support legislation that would provide transparency, accountability, and increased protections to address ESAM in the workplace.

Conclusion
We thank the administration for the opportunity to provide comments on the impact of ESAM on women workers, particularly women of color and low-paid women workers. As demonstrated above, the use of ESAM in the workplace does raise concerns regarding discrimination, job quality, and employment and labor rights. We look forward to working with the administration
to address these challenges. Please contact Adrienne DerVartanian, Senior Counsel, Workplace Justice and Education, at adervartanian@nwlc.org, with any questions.

Sincerely,

Adrienne DerVartanian  
Senior Counsel, Education & Workplace Justice  
National Women’s Law Center

Gaylynn Burroughs  
Director of Workplace Equality & Senior Counsel, Education & Workplace Justice  
National Women’s Law Center

Julie Vogtman  
Director of Job Quality & Senior Counsel, Education & Workplace Justice  
National Women’s Law Center

Emily Martin  
Vice President for Education & Workplace Justice  
National Women’s Law Center
Artificial Intelligence (AI) and its impact on workers through management and surveillance is not a new subject for the United Food and Commercial Workers International Union (UFCW), and its 1.2 million members in the grocery, retail, and meat processing industries. UFCW members have been experiencing electronic surveillance and automation for years. As the nation’s largest private sector union, with members in all 50 states, our members and local leaders see the problems caused by the emerging threat of AI every day.

Please see the attached comments from UFCW International President Anthony M. Perrone.

Attachments

UFCW Comments - RFI - Worker Surveillance and AI
June 29, 2023

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington DC 20504

RE: Federal Register Number 2023-12995. Request for Information:
Extension of Comment Deadline Automated Worker Surveillance and Management

Artificial Intelligence (AI) and its impact on workers through management and surveillance is not a new subject for the United Food and Commercial Workers International Union (UFCW), and its 1.2 million members in the grocery, retail, and meat processing industries. UFCW members have been experiencing electronic surveillance and automation for years. As the nation’s largest private sector union, with members in all 50 states, our members and local leaders see the problems caused by the emerging threat of AI every day.

In the grocery industry, cashiers, and pickers for online orders are monitored constantly for their speed, and at the same time experiencing reduction in hours and jobs due to automated and centralized “just-in-time” scheduling practices. In the food delivery industry, workers misclassified as “independent contractors” are constantly monitored and even disciplined for not meeting often unrealistic and dangerous benchmarks. And in retail warehousing, such as Amazon, companies abuse their workplace surveillance systems to monitor workers’ movements and even their union election voting behaviors.

Automated Worker Surveillance and Management in the Retail Food Industry

Automated Scheduling Means Fewer Hours and Less Money for Workers

Workers in the grocery industry are being squeezed by automated management. Workers are expected to do more with fewer hours due to a more precise “just-in-time” centralized scheduling system run by corporate computers that dictate hours to workers throughout the company and their subsidiaries. These systems schedule fewer workers for fewer hours which means that there is less money in the pockets of the workers and less money circulating within their communities.

These systems often cannot be altered by store managers or take the immediate needs of individuals into consideration. Because schedules are set to maximize worker efficiency, they usually do not consider circumstances such as a flu outbreak or inclement weather which may cause multiple employees to miss work.

Lean Staff Plus Enhanced Monitoring Means More Injuries

Anthony M. Perrone, International President
Shaun Barclay, International Secretary-Treasurer

United Food & Commercial Workers International Union, AFL-CIO, CLC
In the past, employers understood the risks and consequences of staffing their stores with skeleton crews. Those consequences were that lean staffing and customer surges would result in less service. Today, however, when this practice is coupled with enhanced monitoring systems, workers feel compelled to maintain unattainable standards to avoid discipline even at the cost of their own health and safety. For years grocery stores have had some of the most sophisticated equipment monitoring both workers and customers to ensure productivity and prevent theft. Everyone in a grocery store is under constant surveillance, and increasingly more and more workers are required to use devices that constantly monitor their movements.

Cashiers or checkout clerks are monitored by the number of items they scan in an allotted amount of time. The pressure to achieve these benchmarks means over time workers often develop repetitive motion injuries. This is because time standards set by the company do not take best practices for injury protection into consideration. The workers who go through a store to fulfill customer’s online orders, known as pickers, are timed and may experience more injuries as a result. Department heads scanning their inventory have complained that time spent helping customers is not factored into the time allotted for them when using automated inventory systems. Stock crews, who work with sharp knives and spend their shifts lifting heavy objects, are timed in how quickly they can fill their stores shelves which also exposes them to injury.

All of the existing hazards in grocery and retail stores are compounded by the problems of automated scheduling. Previous scheduling systems allowed for moments of “down time” throughout the day where the work slowed but the number of employees working did not change. This provided natural rest periods where even though workers are on the clock and working there is significantly less strain on their body. With more precise scheduling designed to eliminate all down time, workers are in more frequent unnatural movement, exposing them to greater risk of injury. Of course, this risk of injury is even worse when planned lean crews face more customers or have fewer workers than anticipated due to unforeseen circumstances.

Adding Insult to Injury: Automated Scheduling Led to Historic Wage Theft

In 2022, Kroger instituted a new centralized time keeping and payroll system called “My Time” that has been a complete disaster and has led to unfair labor practices, class action lawsuits, and class action grievances. Kroger workers have reported not getting contractual overtime pay, being overcharged for insurance premiums, and going weeks without any paycheck.

UFCW Local Union No. 876 in Michigan filed a class action grievance for over 500 workers. Among these cases, there was a member who was not paid for over three months, which factored into their decision to leave the company. The local union ultimately resolved many of these grievance issues by working with Kroger to do an audit and get members the pay they earned. There are still issues with this system, so the local union set up a special reporting system just to deal with these types of problems.

1https://www.cdph.ca.gov/Programs/CCDPHP/DEODC/OHB/HESIS/CDPH%20Document%20Library/cashiers.pdf
UFCW Local Union No. 951, also in Michigan, experienced similar problems and had so many grievances filed because of “My Time” that they had to set up a special hotline to address them all. In Ohio, UFCW Local Union No. 75 had a class action grievance representing over 100 workers. The local union also noticed that the system was not processing vacation requests accurately.

In Virginia, UFCW Local Union No. 400 has filed a class action lawsuit alleging that the company engaged in wage theft. Members’ claims varied from missing an entire paycheck to being overcharged for insurance premiums.

In the past when such problems occurred and were caught, workers and their union representatives had the ability to address these issues at the store level with managers who had the ability to correct these mistakes and make workers whole for any losses. Now, members go months without pay while this issue is addressed in courtrooms, NLRB hearings, and arbitrations.

**Misclassified Gig Workers Are Not Just Employees – But Constantly Surveilled and Managed by Automated Software**

In 2019, during a hearing from the U.S. House Committee on Education and Labor Subcommittee on Workforce Protection, a gig worker from California named Maria Crawford gave the following testimony on her experience with automated management and surveillance.

“My phone will alert me when a customer places an order, giving me the opportunity to review it on my screen before I accept it. Sometimes I’m not told where to deliver the groceries to until after I accept the batch. I’m only told where to purchase groceries from and how far the delivery is from that store. Since I get dinged for passing on too many orders, I am often pressured into taking jobs that pay me very little money and in some extreme cases may even COST me money after factoring in things like fuel and wear and tear on my car.

I then rush through my grocery store as fast as I can since my time is monitored. If the customer orders an item that is out of stock, I have to message them about an adequate replacement item and hope that they respond in an adequate amount of time. If they take too long to respond, my delivery could be late, which could negatively impact my customer rating.

The app on my phone dictates my ability to take orders. It constantly tracks me. It sets my pay. It times my work. It has the ability to discipline me. While there is a way to appeal discipline, I fear retaliation as the process is vague and inconsistent. I feel as though I have less control over my work now, than in my previous job when my employer rightly classified me as an employee!”

Maria Crawford’s experience represents the struggles of many app delivery drivers who face the challenges and safety hazards of constant computer surveillance. In addition, she is misclassified as an independent contractor rather than an employee so lacks the protections of our federal labor laws like minimum wage and overtime protections. Misclassified gig workers like Ms. Crawford are unable to enforce health and safety standards since she technically has no employer, and she cannot even legally join a union to collectively bargain the supposed “contract” by which she is employed.

It is alarming to hear her talk about being rushed to complete her work – however sadly it is not surprising. Gig workers in food delivery and ride-hailing services, according to the Bureau of Labor Statistics (BLS), are among the deadliest places to work in the United States. Because these app-based jobs monitor every single second while a worker is on the clock, and because these apps have the ability to punish these workers, it is no wonder that drivers are forced to constantly divert their attention from the road. This endangers the workers as well as those around them. These apps are also interactive which means a customer can take a call and text a driver while they are driving, again diverting their attention from the road. These apps knowingly put their workers in harm’s way and have created one of the most dangerous jobs in the country. Delivery drivers including those who work for gig employers account for 1,005 out of all 5,553 workplace deaths according to the BLS. This means that delivery drivers are at greater risk for injury or death than construction workers or police officers.

The risks and fatalities delivery drivers face are not limited to traffic accidents. Delivery drivers are at greater risk of assault than other workers. There have been 80 murders of gig workers reported between 2017-2022. A Pew Research Center poll found in 2021 that thirty-five percent of gig workers have felt unsafe on a job, while nineteen percent experienced unwanted sexual advances. This is important to note, because the constant surveillance workers endured while on the job ONLY exists to ensure their productivity – and is not utilized to guarantee their safety.

Amazon – Warehouses of the Future, Worker Safety, and Union Busting Standards of the Past

There is no company that does a better job of illustrating the risk to workers of “just-in-time” lean scheduling and technology to punitively monitor workers than Amazon. Amazon has mastered eliminating any sort of down time with their now infamous “time off task” metric, even monitoring worker bathroom breaks. It is no wonder the company has injury rates more than twice the rate of other warehouse workers and why the company faced criticism for widespread allegations of workers urinating in bottles to avoid discipline.
While these practices may have started to improve efficiency, they are now more often used for union busting. When workers started unionizing at Amazon, the company used their worker surveillance equipment to disrupt organizing efforts. UFCW-RWDSU organizers noted that Amazon did many of the typical things we see in union busting campaigns: surveillance at union organizing meetings, uniformed off duty cops hired as security for the company, and other unfair labor practices. What was unprecedented was how they tracked voting in the union recognition election. Amazon placed a mailbox to collect union election ballots within their facility that had several cameras on it at all times linked to computers with facial recognition software. The mailbox was also covered in anti-union propaganda. They then instructed all their workers who they believed were voting against the union to submit their ballots there. Management knew in real time who among the anti-union workers had voted and were able to turn out those who had not yet.

Unions Are the Most Effective Solution Against AI Management and Surveillance

UFCW and its members have been experiencing AI and automated management for years, and every year there is more of it. It is important to know, however, that when workers have a union, they have a voice in how automated management and surveillance is used. In addition, they have a process by which they can grieve any violations of the contract or of the law and ensure they are fully paid and made whole. Workers without unions, especially those misclassified gig workers who are not even legally allowed to join a union, do not have that voice. Unions like UFCW are the best balance to unfair and unjust automated worker surveillance and management.

Sincerely,

International President

(b) (6)
My name is Mohamed Farah Hassan. I have worked at an Amazon warehouse in Minnesota for seven years. I am an immigrant from Somalia and I have an English language barrier. I am also a member of The Awood Center, where the East African Community learns, defends our rights at work, and builds East African worker power. We are a worker-led organization dedicated to educating, organizing, developing leadership and mobilizing to improve the economic and political life of the community and all working people.

At Amazon, we are constantly monitored and our productivity is measured, but we often do not know what the company goal is, or what we are expected to do as individual workers. For instance, a manager might tell me, “you have to reach a goal of 100 for an hour,” but we do not know how this is calculated and we are not told starting from what level. This uncertainty, combined with uninterrupted surveillance and pressure makes us constantly worried, both at work and at home. You are constantly thinking about this goal you have to meet, and you know you are being tracked by the minute. Sometimes the worry is so great you forget about going to the bathroom, taking a break, eating lunch, because all you are thinking about is if you are on track to meeting your numbers.

It is not safe for us to work there. We have very heavy loads and we are expected to complete tasks at unsafe speeds. We get injured because of the fast pace of work. We need public policies that would oversee Amazon and prevent us from getting injured. We feel there is an element of racism, that we are targeted based on our skin color, language, and country of origin. They should be held accountable and be concerned with our safety first.

Most injuries at Amazon happen in November and December, this is when Amazon calls it Prime time and we are expected to do a lot of work. Most of the pain comes from the muscles because of the repetitive motions, and those injuries are hard to recover.
from And you are constantly on the go, you are working like a robot All your manager is telling you is to go, go, meet the goal you are expected to meet. Every six seconds, you are twisting, turning, bending, constantly Just imagine that in an hour Then imagine that if you are already injured Sometimes because it is so busy, when you are injured, you do not realize you were working while in pain because you do not feel it until your shift is over

When you get injured on the job, you get sent to Amcare, they will put some ice on you, and then they will send you back, or send you to their doctors. When they refer us to an Amazon doctor, and you go to their clinic, they will check you, and then tell you to go back to work after a few days, saying you are fine. We go back to work, with the same pain, the same injuries, and nothing has changed.

We have rents to pay, families to care for, so we need these jobs. When you go home after your shift, you are in pain, you are tired and irritable, and you do not have quality time to spend with your family. You are carrying the physical and mental impacts of working so hard and fast while being constantly watched, even at home. This situation sacrifices your family time and weighs on your relationships with the people you love.

We have no job security, we worry a lot about losing our jobs, because we see our coworkers get terminated without notice. I have seen my coworkers get written up for time off task, just for going to the bathroom or taking time to pray. That makes you constantly worried because you do not know when you will be fired. You could work there for 10 years, or you could be brand new there, but the situation is the same: Amazon does not always clearly communicate what they set as goals for you, sometimes it is hard to know if you have reached them or not, sometimes you do not even know you have a warning. The next day you come to work and your badge does not work, that means you have been fired.

Other than Amazon using this productivity data to discipline us and push us to work so hard and fast that we get injured, we do not know what purpose these quotas and minute by minute tracking serve. That is why I have organized with my coworkers for safer working conditions at Amazon, and for the Minnesota Warehouse Worker Protection Act so we know what Amazon expects from us. I am proud that the Act will change the lives of Minnesota warehouse workers. My request to you is to please protect every worker that works in a warehouse.
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0205
Comment on FR Doc # 2023 12995

Submitter Information

Email: [Redacted]
Organization: The U.S. Chamber of Commerce's Technology Engagement Center

General Comment

See attached file(s)

Attachments

Comments_AutomatedWorkerSurveillance_OSTP_Final
us-ai-institute-investing-in-trustworthy-ai-full-report-new_OSTP
June 29, 2023

Alan Mislove  
Assistant Director  
Data and Democracy  
Office of Science and Technology Policy  
Executive Office of the President  
1650 Pennsylvania Avenue NW  
Washington, DC 20504

Re: Request for Information, Office of Science and Technology Policy; Automated Worker Surveillance and Management (88 Fed. Reg. 27,932-27,936)  

The U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC") appreciates the opportunity to submit feedback to the Office of Science and Technology Policy (OSTP) in response to its request for information ("RFI") on "Automated Worker Surveillance and Management." The Chamber would like to reiterate our concerns regarding the inadequate time OSTP provided commenters to compile an extensive review of the prevalence, uses, purposes, and deployment of automated worker surveillance and management systems.

We and other organizations requested\(^1\) on May 24\(^{th}\) a 60-day extension to the comment period. While the OSTP's 14-day extension of the comments was published in the Federal Register on June 20\(^{th}\), this brief extension does not provide parties with the necessary time to conduct a thorough review of this RFI and its attendant issues.

The Chamber recognizes that technology brings significant opportunities to the workplace by providing employees and employers with a powerful tool that enhances their organizations' productivity, efficiency, and security. Automated workplace management can enable many benefits, such as:

- **Preventing Workplace Violence and Enhancing Safety and Security:** AI-based workplace management tools, such as video analytics, work zone intrusion detection, panic buttons, and AI monitoring for abnormalities, enable employers to protect employees from harm and improve emergency response proactively. AI-based management tools can enhance workplace safety by deterring potential criminal activity, including workplace violence\(^2\) and theft, and by identifying breaches and safety hazards. These efforts can help employees feel more secure and protected in their work environment.

\(^1\) [https://www.regulations.gov/](https://www.regulations.gov/)

• **Accident and Illness Prevention:** Many employers have recognized the benefits of AI and automated technologies to reduce risk and identify hazards to eliminate workplace fatalities and injuries. In real-time, smart sensors and wearable devices can help detect potential accidents, ergonomic risks, toxic or combustible liquids or gases, or other hazards. Heat stress monitors using AI to monitor worker data—such as humidity, temperature, and increases in pulse—can reduce risks in high heat or outdoor environments to reduce the risk of heat illnesses. AI-enabled robots can conduct inspections in hazardous environments—such as nuclear power plants, mines, and oil rigs—or spaces with a narrow or confined space profile. This allows for prompt intervention and prevention of workplace injuries, ensuring the well-being of employees.

• **Performance Feedback and Training:** Workplace management, equipped with analytics, can provide objective insights into performance, allowing supervisors to identify areas for improvement and provide targeted coaching, training, and other support. This feedback can enhance professional development, improve employee performance and satisfaction, and help employees achieve their career goals. Workplace management tools can be essential in mitigating potential bias by increasing objectivity.

While there are clear benefits, we understand there are legitimate concerns surrounding the use of the technology. For this reason, employers have been careful to adopt new automated workforce technologies only after a rigorous assessment of the benefits and risks of implementing such tools. Furthermore, employers aim to be transparent about how they use new technologies, establish principles to guide them, and follow existing legal protections for privacy and anti-discrimination. They recognize that engaging in an inclusive dialogue about using new technologies is critical to fostering a culture of trust with employees.

The Chamber, in partnership with Deloitte, surveyed senior-level AI researchers, developers, and company decision-makers and released a report titled “Investing in trustworthy AI,” highlighting ways in which the “benefits of AI applications to workers and consumers can increase trust in AI.” Respondents to the survey indicated that workers could become more confident in using and working alongside AI as they saw it improve their day-to-day work experience, safety, and professional opportunities.

The report further highlights, “Building broad confidence and support for AI technologies requires the effective articulation and demonstration of the benefits that consumers, workers, and the public might see from AI-enabled changes to their day-to-day life and work.” While AI unlocks a wide range of benefits, the report cites specific cases of the

---

economic and social benefits of AI for the workforce. For this reason, we will also submit the report along with this response.

The Chamber remains committed to fostering an environment where innovation and productivity thrive while upholding the well-being of workers. We thank you again for the opportunity to participate in this critical discussion.

Sincerely,

(b) (6)

Director, Policy
Chamber Technology Engagement Center
U.S. Chamber of Commerce
Investing in trustworthy AI
A report by the Deloitte AI Institute and Chamber Technology Engagement Center
Foreword

New technologies drive economic growth, create novel opportunities for society, and often raise new challenges and risks. The Deloitte AI Institute™ and the U.S. Chamber of Commerce Technology Engagement Center (C_TEC) find themselves at the forefront of addressing these challenges; helping their clients and members navigate these opportunities. Artificial Intelligence (AI) is no different, but the impact of AI will likely be more substantial and widespread than most technological innovations, affecting nearly every economic sector and occupation.

AI is already securing America’s critical infrastructure, keeping fraudsters at bay, making access to finance more inclusive, and helping find the cures for diseases. These are merely a few examples of how this technology is changing the world. As it develops, it will continue to revolutionize how we tackle future societal challenges, live our day-to-day lives, and conduct business.

The private sector is the leading researcher, developer, and deployer of AI applications and is constantly discovering new ways that AI can be used for good. Consequently, businesses must be at the vanguard of our national discussions on AI to ensure that it is developed and deployed responsibly and consistent with our shared values and should collaborate with government on appropriate public policies to facilitate this goal. In this report the Deloitte AI Institute™ and the Chamber Technology Engagement Center, jointly seek to illustrate how businesses are thinking about the impact of AI on the economy and society, and how government can better enable trustworthy AI, now and in the future.
What’s inside

1. Executive summary
   - Key survey findings
   - Key policy recommendations

2. Part 1: Challenges and opportunities of artificial intelligence
   - Articulating the benefits and risks of AI
   - Benefits of AI for consumers and workers
   - Risks to consumer and worker confidence in AI
   - Impact of trustworthy AI on economic growth
   - How policy interventions can improve AI trustworthiness

3. Part 2: Solutions to enable AI trustworthiness
   - Support for trustworthy AI innovation
   - History of support for trustworthy AI
   - International approaches to AI strategies
   - Public policies to enable trustworthy AI
Executive summary

Artificial intelligence (AI), broadly defined to include the wide range of statistical methods and computational technologies that enable systems to learn, respond, make decisions, and take actions with increasing autonomy, is rapidly becoming an enabler of growth, and a potential game changer of almost every global industry. The United States Patent and Trademark Office reports that as of 2018, fully 25 percent of all US inventors were using AI technologies in their granted patents. While the potential for the United States of harnessing its AI talent, computing capacity, and private-sector-driven innovation is enormous, AI also brings a unique set of challenges that should be addressed so that concerns over its risks do not dampen innovation, and to help ensure the United States can lead globally in trustworthy AI. The U.S. Chamber of Commerce’s Technology Engagement Center (CTEC) shares the perspective with many leading government and industry voices, including the National Security Commission on Artificial Intelligence (NSCAI), the National Institute of Standards and Technology (NIST), and the Deloitte AI Institute, that government policies to advance the ethical development of AI-based systems, sometimes called “responsible” or “trustworthy” AI, can enable future innovation and help the United States to be the global leader in AI.

Building trust and confidence on the part of businesses, their customers, their employees, and the public that AI adoption will lead to a positive impact on the economy and society can accelerate the social and economic benefits that can come from AI to maintain global competitiveness. A potential key to the execution of this approach is US government leadership through public investments and common-sense policies that balance a culture of growth and innovation and ensure that AI applications are developed and deployed in compliance with existing laws and in consideration of social, ethical, safety, security, and privacy concerns. Utilizing a survey of experienced leaders in AI innovation, this paper presents key findings and recommendations on risks and opportunities to trustworthy AI and some policy solutions to help promote the development of trustworthy AI. Part 1 of this paper examines opportunities and innovation that can create economic growth and provide social benefits to the United States while mitigating the risks posed by AI that might arise from the irresponsible development and implementation of AI applications. Part 2 of this report investigates a variety of public policy solutions to enable AI trustworthiness and facilitate positive impacts on the US economy and society.

Building trust and confidence on the part of businesses, their customers, their employees, and the public that AI adoption will lead to a positive impact on the economy and society can accelerate the social and economic benefits that can come from AI to maintain global competitiveness.
Key survey findings

Review of current research, consideration of the perspective of leading voices in government and industry, and the survey results support the position that public policies to support AI innovation can provide lasting economic and social benefits for United States citizens and companies. Building a thriving and sustainable AI-enabled economy will likely require sensible policy solutions to encourage innovators to embed concepts of trustworthy AI in the development and deployment of AI systems. A trustworthy AI approach can mitigate risks that might otherwise reduce confidence in AI systems and stifle innovation in this critical sector, while focusing investment on beneficial applications of AI that can lead to economic growth and improved health, safety, and well-being for Americans.
Emphasizing the benefits of AI applications to workers and consumers can increase trust in AI.

Respondents indicated that consumer trust in AI systems could increase as consumers saw personal benefit from adoption of AI technologies, whether as users of AI-enabled systems or as customers of new products and services generated or accelerated by AI:

- 71% believed that consumers would see benefits from the ability of AI to identify patterns or anomalies in complex and diverse data sets.
- 65% noted that consumers would gain confidence in AI as the pace of discovery of new medicines, materials, and other technologies accelerated.
- 56% indicated that consumers would gain trust in AIs that increased efficiency and reduced repetitive tasks.
- 56% suggested that consumers would see benefit from AI technologies that helped them improve the speed and accuracy of their decision-making.
Similarly, respondents indicated that workers could become more confident in using and working alongside AI systems as they saw it improve their day-to-day work experience, safety, and professional opportunities:

- **69%** saw the creation of new types of work, especially higher-value occupations focused on creating, managing, and maintaining AI systems.
- **62%** highlighted improved safety on job sites or in transit due to AI monitoring or control of equipment and vehicles.
- **55%** noted the increased efficiency and reduced repetitive tasks due to AI-enabled automation.
- **52%** suggested workers might see increased wages or improved working conditions associated with higher-value work made available by AI systems.
Development of AI technologies highlights several risks that may lead to less consumer and customer confidence in AI technologies.

When respondents to the survey were asked to indicate which concerns about AI technologies were likely to have a significant impact on reducing consumer and customer trust in AI:

- 68% identified biases influencing decisions made by AIs.
- 66% identified a lack of human accountability or liability for AI decisions.
- 60% identified rogue or unanticipated behavior of partially or fully autonomous agents.
- 56% identified a lack of explainability of AI algorithms.
Public policies can play a significant role in the mitigation of these risks.

Respondents were confident about the ability of the government to influence the direction of AI innovation toward greater trustworthiness, and positive about the impact government policies could have in accelerating growth in the marketplace, mitigating AI risks, and enhancing AI’s benefits.
When respondents were asked about the ability of the government to mitigate risks associated with AI technologies:

- **72%** indicated that the government could mitigate acceleration of social divides between workers with and without AI skills.
- **69%** suggested that the government could encourage accountability for AI decisions.
- **66%** indicated that the government could mitigate unwanted AI biases.
- **66%** highlighted the government’s ability to reduce the impact of potential job loss due to AI-enabled automation.
- **56%** indicated that the government could address issues with the lack of explainability of AI algorithms.
- **50%** believed the government could address the risk of rogue or unwanted behavior from fully or partially autonomous agents.
Respondents
to the survey
overwhelmingly
agreed that the
government could
contribute to
increased consumer
trust in AI by enabling
its benefits:

85%
expressed confidence that
government policies could
increase the likelihood that new
materials, medicines, and other
products would result from AI
innovation.

72%
highlighted that the use
of AI to helpfully identify
patterns or anomalies could
be accelerated or improved
through government
intervention.

68%
of respondents believed
government could support the
removal of subjectivity and
personal bias from business
processes through expanded use
of AI and adoption of more robust
standards and models.

57%
indicated that the
government could support
the ability of AI systems
to make faster and more
accurate decisions.

54%
suggested that the
government could encourage
the use of AI to increase
productivity.
Respondents were also in agreement that government policies could help contribute to increased worker trust in AI technologies:

- **83%** suggested that the government could encourage the use of AI to increase worker safety on job sites or in transit.
- **76%** indicated that the government could encourage the use of AI to remove subjectivity and bias from scheduling, recognition, and promotion processes.
- **75%** suggested that the government could enable the creation of new types of work focused on creating, managing, and maintaining AI systems.
- **62%** indicated that the government could foster the use of AI-enabled automation to increase efficiency and reduce repetitive tasks.
- **60%** indicated that the government could increase the adoption of AI technologies that expanded worker access to higher-value work, potentially leading to higher wages or improved working conditions.
Appropriate government policies could encourage the development of trustworthy AI and accelerate its potential economic impacts.

Respondents expressed confidence that government intervention in appropriate AI public policies could help facilitate the development of trustworthy AI applications.
There was also consensus around specific policies which the government should pursue to support AI innovation:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>70%</td>
<td>70% of respondents supported government investment in fundamental AI research.</td>
</tr>
<tr>
<td>61%</td>
<td>61% of respondents supported increased access to government data sets for training and improvement of AI models to reduce unwanted bias and increase accuracy.</td>
</tr>
<tr>
<td>53%</td>
<td>53% of respondents noted retraining or continuing education programs targeted at adults.</td>
</tr>
<tr>
<td>50%</td>
<td>50% of respondents encouraged the government to invest in interoperability standards for edge AI hardware and devices.</td>
</tr>
<tr>
<td>64%</td>
<td>64% of respondents supported government encouragement for establishing industry-led, voluntary consensus-based standards for the performance and reliability of AI algorithms.</td>
</tr>
<tr>
<td>54%</td>
<td>54% of respondents supported government policies to support open-source tools and frameworks to enable development of new AI technologies.</td>
</tr>
<tr>
<td>52%</td>
<td>52% of respondents identified establishing or supporting existing international partnerships to promote common frameworks for AI use and deployment.</td>
</tr>
<tr>
<td>50%</td>
<td>50% of respondents identified curricula for youth to promote AI skills and career selection.</td>
</tr>
</tbody>
</table>
Emphasizing federal investments in AI research and development will lead to significant benefits for AI innovation.

When asked to prioritize AI among government R&D investments, respondents overwhelmingly supported increased investment:

- 43% of respondents supported much more investment.
- 46% of respondents expressed support for somewhat more investment.
Respondents generally believe that government investments in AI R&D can help facilitate the development of trustworthy AI applications:

- **97%** of respondents indicated that government investment could influence the direction of AI innovation to at least “a small” extent.
- **83%** of respondents agreed that government investments to a great or some extent enable trustworthy AI innovation.
- Only **3%** of respondents believed that government investments could pursue this objective to a little to no extent.
Emphasizing federal investments in AI research and development will lead to significant benefits for AI innovation.

Respondents generally agreed that government investment was best targeted at earlier stages of AI innovation:

- 61% advocated for government investment in fundamental research.
- 44% suggested that government investment was useful to early-stage startups.
- 31% indicated that government investment was helpful in the transition of early-stage technologies to commercialization.
- 20% suggested that government investment was valuable in the continuing development of established products.
Respondents were also interested in working with the government and were generally open to participating in government investment programs in AI innovation:

64% of respondents were extremely or slightly willing to receive government funding for AI.

Only 10% of respondents expressing unwillingness to accept government funding for AI.

The gap between high willingness to participate in government investment programs and the low number of respondents currently engaged in such programs points to a potential opportunity to increase availability, accessibility, and visibility of government funding to private companies and thereby encourage further AI innovation.

As demonstrated in Case Study 1 of this paper, the economic impact attributable to AI is estimated between $447 billion and $1.43 trillion over five years, which could be accelerated by increased government investments in AI R&D.

The economic impact attributable to AI is estimated between $447 billion and $1.43 trillion over five years, which could be accelerated by increased government investments in AI R&D.
Key policy recommendations

The U.S. Chamber’s Technology Engagement Center has previously proposed\(^3\) that the federal government can best enable trustworthy AI innovation in the United States through the establishment of a national data and AI strategy, which among a number of recommendations includes leveraging federal resources to accelerate innovation, model responsible AI implementations, and support the American workforce in developing AI skills. The survey conducted in support of this paper broadly supports that previous proposal, and highlights specific opportunity areas for policymakers to consider.
Support the development of standards for AI trustworthiness, to guide AI innovation in a responsible direction. Specific public policies to support this approach include developing industry-led, voluntary consensus standards for AI trustworthiness, and an AI risk management framework to assist private sector developers and users in assessing trustworthiness.

Creation of, or support of existing, international partnerships to promote trustworthy AI for the use and deployment of AI technologies with foreign commercial partners and to advocate for US standards internationally, including through digital trade agreements.

Leverage federal resources to accelerate innovation, with specific focus on investing in fundamental research in AI, encouraging the use of shared computing resources, and improving access to government data sets for the development, and training of new AI models.

Model responsible AI implementations in government through e-government applications that serve citizens, the applications used internally by federal agencies, and the development of novel AI applications to address public crises such as the pandemic and climate change and through establishment of procurement processes for trustworthy AI technologies.

Support the American workforce in developing AI skills, including curricula for youth to promote AI skills and career selection, and retraining or continuing education programs targeted at adults to assist in transitioning to job roles that require AI skills.
Part 1: Challenges and opportunities of artificial intelligence

Overview

Why is trustworthy AI important?
The social and economic opportunities of AI in America are enormous, but the confidence of American consumers, workers, and the general public in AI innovation will likely be crucial in unlocking these opportunities. According to Edelman’s 2021 Trust Barometer Tech Sector Report, AI is only trusted by 45 percent of the public in the United States. If the public’s concerns about the risks of AI outweigh their perception of the benefits, the adoption of AI technologies may slow, the private sector may be disincentivized from investing in and utilizing AI, and potential benefits from the widespread adoption of AI applications may not be fully realized. Ensuring that AI technologies evolve and are deployed in ways that consumers and workers are able to reasonably trust is likely a crucial step in building a thriving AI-enabled economy.

What is trustworthy AI?
Many leading voices in industry and government are already aligning around a similar set of ideas as to what constitutes trustworthy AI. Trustworthy AI, also known as ethical or responsible AI, share common themes such as fairness, transparency, and accountability in the development and use of AI applications. Incorporation of these conceptions into the broader national strategy for AI may be essential to realizing the opportunities of the AI-enabled future and maintaining US global leadership in this critical set of technologies.

Ensuring that AI technologies evolve and are deployed in ways that consumers and workers are able to reasonably trust is likely a crucial step in building a thriving AI-enabled economy.
In 2019, the U.S. Chamber of Commerce published ten principles intended to help ensure a stable policy environment that fosters innovation and trust in AI, advocating that:

1. Trustworthy AI be developed as a partnership between government, private sector, academic, and civil society;
2. Existing rules and regulations be leveraged to avoid creating a patchwork of subnational AI policies and to advanced sound and interoperable practices;
3. Risk-based rather than prescriptive approaches be taken to ensure that the highest risk use cases receive the most scrutiny;
4. Investment in public-private partnerships for basic AI R&D be supported in the context of flexible governance frameworks to drive needed advancements;
5. Workers should be supported in gaining needed AI skills and adapting to changing workforce needs;
6. Government data should be made more open and accessible to accelerate the training of AI models;
7. Robust but flexible data protection regimes should be maintained to enable AI development while protecting personal privacy;
8. Intellectual property frameworks that protect and promote innovation should be supported;
9. Data should be free to flow across borders; and,
10. Industry-led, consensus-based international standards should be acknowledged, developed, and promoted through international standards bodies.\(^5\)
Deloitte’s six dimensions for trustworthy AI™

These dimensions recommend that AI-enabled systems are:

1. **Fair and impartial**
   AI systems should make decisions that follow a consistent process and apply rules fairly, as well as incorporate internal and external checks to remove biases that might lead to discriminatory or differential outcomes, to help ensure results that are not merely technically correct but considerate of the social good.

2. **Transparent and explainable**
   AI systems may not operate as “black boxes”; all parties engaging with an AI should be informed that they are doing so and be able to inquire as to how and why the system is making decisions.

3. **Responsible and accountable**
   The increasing complexity and autonomy of AI systems may obscure the ultimate responsibility and accountability of companies and human beings behind the decisions and actions of these systems; policies should be in place to clearly assign liability and help ensure that parties impacted by AI can seek appropriate recourse.

4. **Robust and reliable**
   Just as we currently depend on the consistent performance of human professionals to help ensure that our daily activities are safe and healthy, we should be able to depend on equivalent or even greater reliability as we enable more of our systems with AI.

5. **Respectful of privacy**
   As AI systems often rely on gathering large amounts of data to effectively accomplish their tasks, we should ensure that all data is gathered appropriately and with full awareness and consent, and then discarded or otherwise protected from further, unanticipated use.

6. **Safe and secure**
   As AI systems take greater control over more critical processes, the danger of cyberattacks and other malefices expands significantly. Appropriate security measures should be put in place to help ensure the integrity and safety of the data and algorithms that drive AI.
The private sector has been a long-term leader in articulating and advocating trustworthy and responsible AI. In 2019, the Chamber Technology Engagement Center published ten principles intended to help ensure a stable policy environment that fosters innovation and trust in AI (see inset on page 23). Also, the Deloitte AI Institute has articulated six dimensions for trustworthy AI to guide the responsible development, implementation and governance of systems that utilize artificial intelligence. Deloitte’s Trustworthy AI framework’s dimensions were designed to preserve the ethical integrity of AI-enabled systems through their design, development, deployment, and ongoing operation.

Many other individual companies that market core AI technologies or produce AI-enabled software, including Microsoft, IBM, and Google, have also developed frameworks or guidelines for the implementation of AI within their products, as well as recommendations for how customers can deploy their products in a responsible manner. In addition, other organizations, such as the Partnership on AI, a consortium of industry, academic institutions, and public-interest groups, have also proposed a set of eight tenets for the development and deployment of AI technologies. These tenets include engagement of stakeholders and communities in technology development, protection of the privacy and security of individuals and their data, commitment to the deployment of robust, reliable, trustworthy and secure AI systems, and the principle that AIs must be understandable by and explainable to individuals.

Independent government commissions have pursued similar approaches. The National Security Commission on Artificial Intelligence (NSCAI), a Congressionally-established Commission, released their final report in March 2021 that affirms establishing “justified confidence” in AI systems is crucial to the long-term technological competitiveness of the United States. The report notes, “If AI systems routinely do not work as designed or are unpredictable in ways that can have significant negative consequences, then leaders will not adopt them, operators will not use them, Congress will not fund them, and the American people will not support them.”
NSCAI’s principles on justified confidence in AI systems

The report goes on to articulate five key principles for establishing “justified confidence” in the development and deployment of AI systems, resulting in what it calls “Responsible AI”:

1. Robust and reliable AI systems, especially those related to perception and classification, must be interpretable and explainable, minimizing false positives and negatives and the impacts of bias originating from their design or their data sets.

2. Humans must remain essential parts of AI systems, and appropriate information must be conveyed to enable humans to partner effectively with AI systems to augment decision-making, while avoiding cognitive overload and the resulting tendency to over- or under-trust the systems.

3. Testing and evaluation, verification and validation standards must be put in place to ensure that AI systems are performing as intended.

4. Organizations must have full-time, dedicated leaders with deep subject-matter expertise in artificial intelligence and the risks present in designing and deploying AI-enabled systems.

5. Accountability policies must be evolved to address the unique characteristics of AI systems, and individuals must have reasonable pathways to raise concerns about irresponsible practices or to appeal the actions of AI systems that have caused harm.
Finally, the federal government has also sought to conceptualize trustworthy AI. In November 2020, the Office of Management and Budget (OMB) issued a memorandum on the “Guidance for Regulation of Artificial Intelligence Applications” for the heads of federal agencies that informs the development of regulatory and non-regulatory approaches for AI. The Guidance outlines ten principles for the responsible development of AI applications through the federal government’s role as a regulator, including increasing public participation in rulemaking, ensuring that all actions are informed by high-quality scientific information, weighing risks and costs against the potential for innovation and benefits, and considering the impacts AI may have on fairness, discrimination, safety, and security. In addition, the federal government is pursuing trustworthy AI concepts through the development of standards. In August 2019, the National Institute of Standards and Technology (NIST) published a plan entitled “US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools,” (Plan) in response to a 2019 executive order that intended to help ensure that the United States remains a leader in AI through engaging standards development for AI technologies. The Plan notes that:

“Today, the ability to understand and analyze the decisions of AI systems and measure their trustworthiness is limited. Among the characteristics that relate to trustworthy AI technologies include accuracy, reliability, resiliency, objectivity, security, explainability, safety, and accountability. Ideally, these aspects of AI should be considered early in the design process and tested during the development and use of AI technologies. AI standards and related tools, along with AI risk management strategies, can help to address this limitation and spur innovation.” —NIST

NIST’s Plan has been followed up by additional publications and workshops focused on specific topics such as AI explainability, bias, and trustworthiness. Congress has also tasked NIST, through Division E of the Fiscal Year 2021 National Defense Authorization Act to further support the development of AI standards for trustworthiness. The role played by NIST will ultimately not just assist federal agencies but likely also the private sector in developing common conceptions of trustworthy AI.

As the United States continues to develop its national approach to lead on trustworthy AI, we should consider incorporating these insights from private and public sector institutions to guide AI responsibly to help ensure that the concerns of consumers, workers, and the public about AI innovation are addressed. Development of this approach can be accelerated by leveraging the substantial work already completed by the federal government in collaboration with the private sector and other key stakeholders.
Articulating the benefits and risks of AI innovation

The exponential rate of change enabled by AI is already visible across numerous facets of our society and economy. A 2020 survey by Cognilytica showed that 40 percent of business decision-makers already have one or more AI projects in place, and fully 90 percent plan to have an in-progress AI implementation within two years.¹⁴ The use of AI in the pharmaceutical industry to identify new compounds and accelerate production processes to make possible the rapid time-to-market of mRNA vaccines for COVID-19¹⁵ is just one prominent example of how AI-enabled business transformation is yielding benefits today. Achieving a culture of AI innovation that yields medical breakthroughs and addresses pressing global challenges will require governments and the private sector to cooperate to assure citizens, workers, and the public that AI technologies are being developed and deployed appropriately. This section discusses and examines the commonly cited benefits and risks of AI in the context of how they contribute to perceptions of trustworthy AI.
Benefits of AI for consumers and workers

Building broad confidence and support for AI technologies requires the effective articulation and demonstration of the benefits that consumers, workers, and the public might see from AI-enabled changes to their day-to-day life and work. While there are a wide range of benefits unlocked by AI, some of the commonly cited economic and social benefits include the following:

Improved speed and accuracy of decision-making

The ability to prevent and respond to cybersecurity threats remains a critical challenge faced by both governments, the private sector, and the public at large. BlackBerry’s AI-driven cybersecurity tools use AI to improve cyber threat protection and remediation by quickly reviewing large volumes of cyber incident data, including information drawn from previous malware attacks, while leveraging machine learning and automation to identify potential threats.6 AI and machine learning can serve as a force multiplier by helping outnumbered security teams automate tasks that usually require valuable time and resources.

Removal or mitigation of biases and subjectivity from high-impact decisions

Decisions with significant personal and professional impact, such as hiring and promotions, determination of creditworthiness, vendor selection, and admittance to institutions of higher education, can be influenced by unwanted bias, caused by the conscious or unconscious preferences of decision-makers. AI can assist in identifying and mitigating those biases, bringing objectivity to decisions that are today highly subjective today, and making complex decisions such as career paths more predictable and manageable for individuals. In 2019, the California State Assembly passed ACR-125, which encourages the state of California to invest in and support the development of AI and algorithm-based hiring technologies with the capacity to reduce bias and discrimination related not only to protected characteristics such as race or sex but also unprotected characteristics such as socioeconomic status or previous incarceration.17
Improved speed of innovation and pace of discovery of new medicines, materials, and technologies

Consumers and the public stand to benefit enormously from the faster rate at which AI-enabled processes can improve the quality, durability, and cost of existing goods, as well as from the introduction of entirely new products to benefit consumers. AI innovation promises novel medicines, improved flavors, more energy-efficient electronics, and a host of other small and large improvements to goods and services enjoyed every day. Project Dreamcatcher, a collaboration between Autodesk and General Motors, generates thousands of options for part designs that address constraints and performance criteria input by designers, resulting in novel, often complex structures able to then be built with additive manufacturing techniques.18

Increased scale of operations through deployment of partially or fully autonomous agents

AI enabled agents can operate continuously, accelerating the pace at which product selection, packaging, transportation, and delivery can be accomplished, whether through the use of robotic assistants in warehouses or automated vehicles or drones in delivery. Ultimately, improvements in business processes can lead to significant benefits for consumers. Amazon leverages over 100,000 autonomous guided vehicles within its warehouses to augment the capacity of its human workforce and meet the expectations of its Prime customers for fast and accurate deliveries.19

Increased ability to detect patterns or anomalies in complex data sets or across diverse sources of input

Fraud and other types of illegal activity cost consumers both directly and in the form of higher costs across all goods and services.20 The Nilson Report indicates that in 2019, payment fraud alone amounted to over $9.6 billion in losses for US consumers.21 Better detection of anomalous behavior could stop this activity early and limit the consequences of fraud. Similarly, small, day-to-day changes from poor diets or posture could be detected and addressed earlier, before long-term and high-impact health changes could result; a 2018 study showed that small, positive changes in day-to-day lifestyle choices could add as much as 12 to 14 years of additional life expectancy for Americans.22 Verizon uses pattern recognition AI to predict network failures from temperature, weather, and equipment sensor data, significantly reducing the occurrence of network downtime experienced by customers.23

New types of work and specialized occupations focused on creating, managing, and maintaining AI systems

New types of work stemming from AI include jobs directly focused on the development and deployment of AI systems, such as designing and training models or implementing new AI applications, but also include a range of indirect opportunities that come from gathering and normalizing data with which to train models, testing and validating the performance and robustness of AI applications, and training workers to work alongside AI systems that augment their jobs. As AI applications increasingly reach edge and device computing, the development and installation of new hardware environments such as camera systems, listening devices, and temperature sensors could create a range of field services, “blue collar” and “white collar” jobs similar to those created by the widespread deployment of communications networks in the previous century.24
Reduction of repetitive tasks due to AI-enabled automation

On an industrial scale, AI systems can assist in sorting agricultural products, identifying damaged or inferior goods during their journey through an assembly line, automating the formatting and creation of many types of digital documents and assets, and even fielding common support and customer services queries. Within the home, AI systems can reduce chores, and the planning and scheduling burdens associated with managing a household, and support for personal development activities such as improved health and fitness. For example, Amtrak’s “Julie” AI-enabled chatbot has answered over 5 million common customer queries, saving more than $1 million in customer service expenses annually.\textsuperscript{25}

Increased wages or improved working conditions associated with higher-value work made available by AI systems

Many of the jobs that are created by AI are more likely to involve quantitative skills, manipulation and management of data, and more specialized maintenance and field service activities, all of which have historically been associated with higher wages.\textsuperscript{26} The Montreal Economic Institute notes that AI is likely to enable workers to migrate to higher-value tasks due to the effects of human-machine complementarity observed in previous cycles of automation, as well as by enabling less experienced workers to become more productive more quickly.\textsuperscript{27}

Improved safety on job sites or in transit due to AI monitoring or control of equipment and vehicles

AI systems, especially when combined with sensors, can be deployed to monitor hazardous conditions that might be caused from faulty equipment or exposure to noxious chemicals. These systems can also be put in place to assist workers in maintaining safe distances from operating equipment, or to track wakefulness of operators of heavy equipment or drivers of field service or delivery vehicles. In the long term, automated vehicle technology may reduce accidents and minimize worker exposure to risks associated with transportation. For example, in the United Kingdom, Cisco has deployed AI-SAFE, an AI-enabled computer vision system to help detect whether workers are wearing appropriate protective equipment.\textsuperscript{28}

Many of the jobs that are created by AI are more likely to involve quantitative skills, manipulation and management of data, and more specialized maintenance and field service activities, all of which have historically been associated with higher wages.
Survey respondents were asked to evaluate these benefits in terms of their positive impact on the confidence of consumers and workers in AI. When survey respondents were asked to identify which of these benefits would have an impact on improving consumer trust in AI systems, AI’s role in identifying patterns in complex data and accelerating the pace of innovation had the highest support. Pattern and anomaly detection, identified by 71 percent of respondents, helps consumers by helping them detect the “needle in the haystack,” and includes applications that can track and improve physical health, monitor and proactively recommend better financial choices, and improve personal safety. 65 percent of respondents identified access to new products and solutions generated by AI as another key driver of consumer trust. A majority of respondents also signaled that AI’s ability to increase productivity (56 percent of respondents) and improve the speed and accuracy of decision-making (56 percent of respondents) could also improve consumer trust in AI systems. Consumers benefit from better productivity both in terms of reduction of their own work, and in faster and higher-quality service in their interactions with AI-enabled businesses and governments. Similarly, consumers may both use AI directly to improve their personal decision-making, such as the selection of entertainment options, and benefit from better decision-making in the retail context, such as improved assortment planning and display of products.
Similar trends were found in responses regarding worker or employee trust in AI systems. While some have concerns about job loss stemming from automation—a 2019 CNBC poll indicated that 27 percent of American workers feared the loss of their job due to AI-related automation within five years—respondents indicated that workers were more likely to embrace AI systems that had positive impact on their careers and working conditions. 69 percent of respondents identified the creation of new types of work as likely to build worker trust in AI, as this could directly mitigate concerns about automation and demonstrate the potential for future careers working alongside AI systems. This is also supported by 55 percent of respondents noting increases in productivity through reductions of repetitive work resulting from use of AI technologies and 52 percent of respondents who express support for the idea that increased wages and improved working conditions derived from AI could increase trust. This is a pattern seen over the past decades with the rise of the information technology: few workers today fear being replaced by a personal computer, but many make use of computers to perform professional tasks that were scarcely imaginable fifty years ago. Respondents also strongly emphasized the value of AI-driven improvements to work safety in building worker trust in AI systems, through improved safety on job sites due to AI monitoring or control (62 percent of respondents). This supports prior studies showing that job satisfaction and general engagement in all work tasks are highly correlated to perception of the safety of the work environment.
Risks to consumer and worker confidence in AI

Despite the many benefits of AI to consumers and workers, some have raised concerns over the risks posed by certain AI applications. Some of these applications, for example, may have unwanted bias through flawed or unrepresentative data, and consumers may be subject to the decisions of “black box” systems without understanding how and why they were impacted. As discussed earlier, some also fear job losses due to increased AI-enabled automation, and AI may exacerbate existing social and economic divides between workers with different skillsets. Finally, some may be concerned about rogue or unanticipated behavior from partially or fully autonomous agents such as robots or software systems, and are cognizant pertaining to risks to critical infrastructure, public safety, and human health. The survey asked respondents about several commonly cited risks posed by AI systems including:

Biases influencing decisions made by AIs

Perceived, and actual, discrimination by AI systems undermines the confidence individuals have in whether they are being given a fair opportunity when AI is involved. Bias has the potential to be introduced, intentionally and unintentionally, throughout the lifecycle of the AI system, including during deployment. Intentional or unintentional discrimination against specific types of people may occur in the following situations: hiring AIs trained on resumes primarily submitted by men may disadvantage women who apply for jobs, and visual AI systems trained on younger faces or individuals with lighter complexions may misidentify or fail to recognize older faces or individuals with darker complexions.

Lack of human accountability or liability for AI decisions

A key challenge will be to determine how to assign responsibility when AI systems are involved and to what extent AI systems will be subject to the same legal frameworks regarding non-AI systems. Some existing incentives for entities to design and maintain systems in a safe and responsible manner hinge on legal and financial obligations for accidents and errors. Like all technological systems, AI systems are ultimately designed and deployed by humans, so human accountability for the impacts of AI systems is an important aspect of AI risk mitigation.
Rogue or unanticipated behavior of partially or fully autonomous agents

As the use of AI becomes more widespread, workers, consumers, and the public should have assurance that AI systems are safe. A patient seeking medical treatment in a hospital should be confident that an AI-enabled surgical system is properly controlled, and a worker who depends on AI-enabled system to safely maintain temperatures or power levels should have certainty they will not be injured by an unexpected or unwanted AI decision.

Lack of explainability of AI algorithms

The “black box” nature of certain AI models could feasibly lead to unfair decisions and confusion for workers and consumers. Insufficiently explainable AI applications can create situations where it is difficult to determine why or how the overall system operates. As noted by NIST’s “Four Principles of Explainable Artificial Intelligence” explainability is necessary in many contexts to ensure social acceptance of AI applications and be transparent to the public.31

Potential loss of jobs due to increased AI-enabled automation

While the AI economy will likely create many new jobs and occupations, the introduction of AI systems may require some workers to transition to new jobs. A 2019 Brookings report found that 25 percent of all American jobs were at high risk of elimination due to automation and AI. In previous cycles of technology transformation, job losses were concentrated among lower-skilled workers, but in the near-term the transition to an AI-enabled economy is likely to also affect “white collar” and higher-skilled workers.32

Acceleration of social and economic divides between workers with and without AI skills

As the AI-enabled economy accelerates, a new type of “digital divide” could arise that may negatively impact communities or exacerbate social tensions if access to AI skills is not broadly available, or if wage differentials between AI-augmented work and non-augmented work increase more than is already observed between “high tech” and “low tech” occupations.33

Some may be concerned about rogue or unanticipated behavior from partially or fully autonomous agents such as robots or software systems, and are cognizant pertaining to risks to critical infrastructure, public safety, and human health.
Survey respondents were asked to evaluate whether these risks raised with regard to AI might reduce the trust of consumers and workers in AI systems. When asked to identify which of these risks was likely to reduce trust in AI systems, respondents were especially concerned about biases in decision-making (identified by 68 percent of respondents) and lack of human accountability or liability for AI decision-making (identified by 66 percent of respondents). Consensus was also found around concerns related to rogue behavior of partially or fully autonomous agents and lack of explainability of AI algorithms, identified by 60 percent and 56 percent of respondents, respectively. Some respondents also noted loss of jobs (47 percent of respondents) and acceleration of social and economic divides (37 percent of respondents) as significant risks to overall consumer trust in AI systems.

Among the following concerns related to AI technologies, which do you regard as significant in terms of reducing customer and consumer trust in AI systems?

While AI systems promise substantial benefits, the development and deployment of trustworthy AI also requires mitigating the risks posed by AI. Moreover, the survey data strongly suggests that bolstering the benefits of AI could also improve AI trustworthiness. Overall, this suggests that conceptions of trustworthy AI should consider the risks posed by AI, but also the potential benefits to provide a balanced perspective on the impact of AI.
Impact of trustworthy AI on economic growth

If the risks posed by unmanaged development of AI are left unaddressed, reductions in consumer and worker trust may inhibit the long-term growth and adoption of AI technologies, and discourage the private sector from investing in AI-enabled solutions and limit the benefits of AI and on overall economic growth. The consequences of the inhibition of the AI market are significant, with long-term risks to the ability of the United States to compete globally if it fails to maintain leadership in AI. IDC estimated for instance, that revenues for the AI market are projected to reach $327.5 billion in 2021, which does not even consider the secondary benefits from implementing and utilizing AI systems.³⁴

Respondents to the survey were asked to indicate the relative economic impact of common concerns about AI in the absence of solutions to mitigate them. Overall, the risks of social disruption due to loss of jobs from increased automation and the potential acceleration of social divides between workers with and without AI skills were considered to have the largest economic impact, with 76 percent and 79 percent of respondents, respectively. Also, lack of accountability for AI decisions and concerns over bias also ranked highly, with 64 percent and 65 percent of respondents respectively who acknowledged these challenges indicating that these areas could have a negative economic impact if left unchecked. Overall, untrustworthy AI technologies could negatively impact economic growth, reinforcing the importance of government or non-government solutions in addressing AI risks.
Respondents also indicated that government policies that enable the benefits of AI could have significant positive economic impacts, which indicates that the federal government can contribute to increasing public trust in AI applications. 90 percent of respondents who identified increased speed of innovation as a benefit of AI affirmed that positive economic impacts could result from new beneficial products generated by AI such as improved materials and novel medical treatments reaching the market, demonstrating the wide-ranging positive impact of AI on innovation across sectors. 70 percent of respondents who identified increased productivity as a benefit of AI indicated that this increase in productivity could result in positive economic impacts. In fact, each of the benefits attributed to AI was held by a majority of its identifying respondents to be likely to have a positive economic impact if realized with the support of government investment, including improved speed of decision-making, increased scale of operations, improved pattern and anomaly detection, and reduction of subjectivity and bias in core business processes.

A similar trend was found regarding the positive economic impact of increasing trust in AI on the part of workers. 72 percent of respondents who identified improved worker safety as a benefit of AI suggested that improvements to worker safety resulting from AI innovations could create economic benefits, and 81 percent of respondents who believed that AI would create new types of work indicated that government policies could encourage the AI economy to grow. Also, respondents who indicated that AI could improve the quality of the work experience through mitigating subjectivity in scheduling and hiring processes, reducing repetitive work, and increasing wages and working conditions, generally believed that these benefits could be bolstered with appropriate government policies and could contribute to greater overall economic impact (66 percent, 70 percent and 72 percent of respondents respectively).

A similar trend was found regarding the positive economic impact of increasing trust in AI on the part of workers. 72 percent of respondents who identified improved worker safety as a benefit of AI suggested that improvements to worker safety resulting from AI innovations could create economic benefits, and 81 percent of respondents who believed that AI would create new types of work indicated that government policies could encourage the AI economy to grow. Also, respondents who indicated that AI could improve the quality of the work experience through mitigating subjectivity in scheduling and hiring processes, reducing repetitive work, and increasing wages and working conditions, generally believed that these benefits could be bolstered with appropriate government policies and could contribute to greater overall economic impact (66 percent, 70 percent and 72 percent of respondents respectively).

### Among these benefits, which are likely to have the greatest economic impact if encouraged by government investment or intervention?

While the introduction of AI technologies is already showing significant economic impacts in the United States and abroad, the survey results demonstrate that both risks to AI trustworthiness and the benefits if AI can lead to negative or positive economic impacts. This demonstrates that policy solutions addressing trustworthiness could play a role in strengthening the economic potential of AI applications. The next section discusses what types of government policies are likely to enable trustworthy AI and ultimately increase trust in AI technologies.
How policy interventions can improve AI trustworthiness

While the federal government can pursue a number of different policy options, not every investment or intervention can make a meaningful impact on their intended outcomes and could instead inhibit innovation. Thus, it is important to assess whether specific risks and benefits of AI technologies can be effectively addressed by particular policy interventions.

Survey respondents were first asked to identify the areas of concern around AI most likely to be mitigated or reduced by government investment or intervention. In general, respondents had a highly favorable perception of the ability of public policies to influence the direction of AI innovation through the adoption of trustworthy AI. Respondents who acknowledged the risks of accelerating social divides between workers with and without AI skills largely agreed (72 percent of respondents) that government intervention could mitigate this risk, likely due to perception of government’s existing role in providing social services. Providing accountability for AI decisions and mitigation of AI biases were also seen as meriting government policy interventions, with 69 percent and 66 percent of respondents, respectively, identifying that these risks could be mitigated by government action. Respondents concerned about loss of jobs due to automation and lack of explainability of AI algorithms also exhibited confidence that government could address these issues (66 percent and 56 percent of respondents). Only 50 percent of respondents who had identified the risk of rogue or unwanted behavior from fully or partially autonomous agents believed that government could address this concern, with the somewhat weaker support perhaps attributable to the nature of rogue behavior being unanticipated or resulting from existing oversight mechanisms.
In addition, respondents were asked whether government policy interventions could accelerate or improve the likelihood that some of the potential benefits of AI technologies to consumers and customers could materialize. Broadly, respondents overwhelmingly supported the notion that government intervention could enhance the benefits of AI and thus contribute to increased AI trustworthiness. The vast majority (85 percent) of respondents who had highlighted the potential of AI to create new products expressed confidence that government policies could increase the likelihood that new materials, medicines, and other products would result from AI innovation. 72 percent of respondents who highlighted the benefits to consumer trust in AI from identification of patterns or anomalies indicated that this beneficial use could be accelerated or improved through government intervention, such as expanding the availability of training data sets or open-source models. Similarly, 68 percent of respondents who acknowledged the capacity of AI to build trust by removing subjectivity and personal bias from business processes believed that government policies could be supportive of this goal, again likely in the form of improved training data and models, and through publication and adoption of standards for AI robustness. Respondents were more divided as to whether government policies could improve the ability of AI systems to help make faster and more accurate decisions and increase productivity, but the majority of respondents, 57 and 54 percent respectively, still indicated they could be boosted by government policies.

Among these benefits for consumers and customers, which are the most likely to be accelerated or improved by government investment or intervention?
Respondents who indicated the positive impact of new job creation on worker trust in AI believed that government policies could positively impact the pace and scale at which new jobs could be created. Finally, respondents generally agreed that the benefits of AI that enhanced employee and worker trust in AI could be bolstered by government intervention. Job safety improvements resulting from AI were considered by 83 percent of respondents as a trust-building benefit of AI likely to be accelerated by government policies. Also, 76 percent of respondents who had identified AI in removing biases from hiring, scheduling, recognition, and other traditionally subjective processes agreed that this use of AI could be accelerated by government policies. 75 percent of respondents who indicated the positive impact of new job creation on worker trust in AI believed that government policies could positively impact the pace and scale at which new jobs could be created. Smaller, but still significant majorities, also believed that government could accelerate the reduction of repetitive work, and increased wages and improved working conditions (62 percent and 60 percent respectively).

Among these benefits for employees and workers, which are the most likely to be accelerated or improved by government investment or intervention?

The high degree to which respondents indicated that government has the capacity to invest and intervene in both the mitigation of AI risks and the acceleration of its benefits indicates the importance of advancing public policies centered around trustworthy AI. This support may take the form of federal investments in R&D, the publication and adoption of AI-related standards or other policy opportunities. We explore some of these potential public policies in Part II of this paper.
Part 2: Solutions to enable AI trustworthiness

Support for trustworthy AI Innovation

History of federal government support for trustworthy AI

The federal government has traditionally acted to provide both financial support and the establishment of other policies for the safe and responsible implementation of transformative technologies. In the 1910s, early adoption of automobiles was accompanied by accidents and reckless driving, leading to the National Safety Council’s promotion of safe driving practices and collaboration with industry to introduce innovations such as shatter-resistant windshields by the 1920s.35 This early impetus encouraged later market-led innovations such as steel frames and hydraulic brakes as manufacturers competed to earn the trust of consumers that their vehicles were safe. Automobiles enhanced the American economy in numerous ways, bringing increased mobility to millions of Americans, connecting communities, expanding the speed and opportunity to deliver goods and services between far-flung markets, and fostering dynamic cultures of sport and even art. The impacts of the automotive industry have played out across American society over a period of more than 100 years and the introduction of AI is potentially greater, and we may experience the impacts of AI in a much more compressed timeframe.
The impacts of the automotive industry have played out across American society over a period of more than 100 years and the introduction of AI is potentially greater, and we may experience the impacts of AI in a much more compressed timeframe.

Important activities have already been pursued by both the Legislative and the Executive branches on a bipartisan basis to embed trustworthy AI within a broader AI policy agenda. The federal government should continue its efforts to formalize, promote, and build off existing efforts to advance trustworthy AI. Some of these key activities from the Executive Branch include:

- The National Science and Technology Council (NSTC), part of the Office of Science and Technology Policy (OSTP), released a National Artificial Intelligence Research and Development Strategic Plan in October 2016 presenting 23 specific policy recommendations for the development and deployment of trustworthy AI systems. This plan was updated in June 2019.

- A number of agencies also participated in a report published by the Executive Office of the President in December 2016 on “Artificial Intelligence, Automation and the Economy” which explored the specific ways in which the government could support private enterprise in ensuring that the “enormous benefits of AI and automation are developed by and available to all.”

- Executive Order 13859, Maintaining American Leadership in Artificial Intelligence, issued in February 2019 and parts of which were codified into law as the National AI Initiative Act of 2020, emphasized the respect for existing laws and national values, and development of trustworthy AI in government that is safe, secure, resilient, explainable, and accountable.

- Pursuant to Executive Order 13859, the Office of Management and Budget (OMB) provided guidance to federal agencies on regulatory and non-regulatory approaches towards AI technologies in a memorandum finalized in November 2020.

- Executive Order 13960, issued December 2020, specified nine principles for trustworthy AI development and deployment within federal agencies, as well as a specified timeline for inventory of existing AI applications that might be inconsistent with these principles.

Congress has also acted to advance trustworthy AI. In the 116th Congress, lawmakers enacted the AI in Government Act to enable the responsible federal government use of AI as well as Division E of the FY 2021 NDAA (National Artificial Intelligence Initiative Act of 2020) to advance US leadership in AI, establish AI R&D programs across the federal government, and lay the foundation to establish AI-related standards. Also, Representatives Will Hurd (R-TX) and Robin Kelly (D-IL) introduced a concurrent resolution in September 2020, recommending a comprehensive national approach to AI including workforce transformation, research and development, national security, and ethical considerations, which was adopted by the House of Representatives in December 2020. As the use of AI applications continues to accelerate, these activities are likely only the beginning of Congressional engagement in AI policy.
International approaches to AI strategies

The United States’ pursuit of AI is not occurring in a vacuum. While the United States was an early leader in AI, the rapid rise of China and other global competitors in this space makes it important for the United States to maintain global leadership in international forums where the rules of the road for the appropriate uses of AI are established. Maintaining global competitiveness in AI should include a continuous awareness of the strides that other nations are making in developing their own national strategies. HolonIQ assembled a list of 50 large economies that had developed their own national AI strategies, but the examples of several key global partners and competitors provide specific insight into the types of comprehensive investment that the United States should make to help remain competitive:

**China**
China’s New Generation Artificial Intelligence Plan targets a domestic AI industry worth more than $150 billion by 2030. Key to China’s strategy is active partnership between the state and its large technology companies and the use of government-sponsored applications to collect and provide data to support the creation of new AI systems. China’s approach of active government intervention in commercial development and expansive regime of digital protectionism is especially important for the United States to counter. The US’s success in AI will demonstrate that democratic states with market-driven strategies for innovation can be equally or more effective in driving innovation and economic benefits.

**Russia**
Russia has been explicit in its commitment to AI as a competitive differentiator of its military technologies, especially the development of autonomous and robotic military platforms, but its broader National Strategy for the Development of Artificial Intelligence identifies key investments that will support its internal software industry and maintain its competitiveness in key sectors such as cybersecurity. The Russian government has supported these efforts by adopting an import-substitution policy that restricts US companies’ access to the Russian software market and supports local rivals.

**European Union**
The European Union, led by the European Commission, is putting regulation at the center of its AI strategy. In April 2021, the Commission published a draft AI law that would subject a long list of AI applications deemed as “high risk” to new requirements. Enterprises would need to undergo a conformity assessment process illustrating their compliance with these requirements in order to place high risk applications on the European market. The proposal is broadly extraterritorial, reflecting the desire of many EU policymakers to export European legal standards globally, as it had done with the General Data Protection Regulation. As part of its broader efforts to advance “technological sovereignty,” EU institutions and Member States are developing new rules relevant to AI, many of which raise concerning questions about the bloc’s commitment to open markets. These include restrictions on cross-border data flows and US cloud computing providers, and a new legal framework for data sharing. Just as it is important for the United States to
While the United States was an early leader in AI, the rapid rise of China and other global competitors in this space makes it important for the United States to maintain global leadership in international forums where the rules of the road for the appropriate uses of AI are established.

demonstrate an economically successful counterexample to the centrally planned strategies used by China, the United States should also address concerns raised by stakeholders about the protection of citizen’s safety and privacy without ceding its competitiveness. As in other areas of digital policy, the EU may choose to prioritize the former at the expense of the latter.

The United States should lead not only in technology and economic growth, but also in values. Establishing norms of trustworthy AI within the American market and internationally should be a core focus of government policies that advance AI technologies. Just as international standards for digital trade, and monetary policy, create a more stable world and a healthier global economy, US leadership in trustworthy AI can maintain open and competitive markets for AI vendors and protect citizens from threats to their privacy, safety, and civil rights at home and abroad.
Public policies to enable trustworthy AI

The United States has a significant opportunity to support the benefits of AI innovations while mitigating concerns over the risks of AI while being a global leader in trustworthy AI. A proactive policy strategy focused on facilitating the development of trustworthy AI could:

• Harness private sector expertise to take a leading role in the development of human-centered AI innovations;

• Foster the emergence of new business opportunities stemming from those innovations;

• Increase the enfranchisement of American workers in the benefits of the AI economy; and

• Build the trust of consumers and the general public that AI innovations offer greater economic and social benefits than risks.

Broadly, this support should be focused on policies that can drive AI innovation in a trustworthy and responsible direction while maintaining a policy environment suitable for innovation. A wide range of policy options exist to increase trust in AI applications given that AI crosses sectors and involves a variety of different inputs such as data, compute power, and a skilled workforce. While there are a number of policy options have been proposed by lawmakers, industry bodies, think tanks, and civil society groups, this paper focuses on solutions derived from in-depth conversations with leaders from industry, academia, and public policy. These solutions particularly focus on standards and frameworks, research and development, the workforce, and leveraging AI in government. Collectively, these solutions can promote innovation, maintain US AI global leadership, and support the growth and competitiveness of American businesses while embracing the trustworthy AI principles that can help address the social, ethical, safety, security, and privacy concerns.

Collectively, these solutions can promote innovation, maintain US AI global leadership, and support the growth and competitiveness of American businesses while embracing the trustworthy AI principles that can help address the social, ethical, safety, security, and privacy concerns.
Respondents were asked about ten different categories of policy solutions that could enable the development of trustworthy AI, which include:

- Fundamental research in AI
- Standards for performance and reliability of AI algorithms
- Access to government data sets for improved training of AI models
- Interoperability standards for edge hardware and devices
- Access to shared computing and cloud resources for developing and training new AI models
- Open-source tools and frameworks to simplify or accelerate development
- Curricula for youth to promote AI skills and career selection
- Retraining or continuing education programs targeted at adults to assist in transitioning to job roles that require AI skills
- Establishment or support of existing international partnerships to promote common frameworks for the use and deployment of AI
- Model the implementation of trustworthy AI systems within government

When respondents were asked about their public policy priorities, a clear preference emerged for three specific interventions. 70 percent of respondents identified fundamental research in AI as an enabler of broader innovation in the marketplace, as businesses and entrepreneurs could leverage public investments in R&D as a foundation for their own R&D (a topic explored more fully in Case Study 1 of this paper). 64 percent of respondents recommended that government support in the development and publication of standards for the performance and reliability of AI algorithms. Industry-driven, voluntary consensus standards are essential components in the design of trustworthy AI that represents a significant cost and effort for an individual business to develop, and collaboration on standards is valuable to ensure consistency in the marketplace. 61 percent of respondents identified improving access to government data sets for the training and improvement of AI models as a top priority, which is important to maximize access to a key ingredient of developing AI applications (a topic explored more fully in Case Study 2 of this paper).
Smaller, but still significant percentages of respondents, 54 percent, 52 percent and 50 percent of respondents, respectively, identified open-source tools, participation in international partnerships and interoperability standards for edge AI hardware and devices as enablers of trustworthy AI development meriting government policy intervention. Also, respondents generally supported education and workforce policy solutions to bolster trustworthy AI, with 53 percent of respondents supporting programs to retrain existing workers and/or provide continuing education for adults, and 50 percent supporting the creation of curricula for youth to promote AI skills and career selection. Finally, 42 percent of respondents supported government investment in shared computing resources such as a national AI research cloud, especially for the computationally intensive task of training new AI models.

Among the following enablers of the development of trustworthy AI technology, which should be targets for government investment or intervention?

Among the following policies and government interventions, which are likely to support trustworthy AI innovation?
Once they had identified investments and interventions that the federal government should make to support the development of trustworthy AI, respondents were then asked to prioritize among the areas they had selected. Supporting the development of standards and fundamental research in AI were most commonly considered higher priorities relative to other possible investments, by 79 percent and 71 percent of respondents respectively. 70 percent of respondents identified interoperability standards for edge AI systems as a high priority, followed closely by expanded access to government data assets for model training, and access to shared computing and cloud resources for developing and training new models (considered as a high priority by 69 and 61 percent respectively).

In addition, modeling the implementation of trustworthy AI systems within government was the highest priority among respondents who had selected this intervention, with 80 percent of respondents noting it should be the highest priority for policymakers. This solution was followed closely by other policies such as development of AI curricula for youth and retraining programs for older workers (considered high priorities by 78 percent and 76 percent of their advocates, respectively). Support for international partnerships, prioritized by 69 percent of respondents, received the lowest support relative to the other solutions, but still retained significant support.

Among these enablers of the development of trustworthy AI technology, which should be the highest priorities for government investment or intervention?
Promote the establishment of standards for trustworthy AI

International, industry-driven, voluntary consensus standards underlie a number of technologies and products, and are often necessary to foster an effective market and can serve as the foundation for future regulations. The long-term development of trustworthy AI likely depends on the establishment of evidence-based standards regarding AI transparency, fairness, explainability, bias, and accountability. Identified as a priority by 64 percent of respondents, the process of developing these standards is often contingent on substantial investments in the core research required to establish effective methods for determining appropriate standards in ways that actually mitigate real-world risk while enabling continued innovation.

The National Institute for Standards and Technology (NIST) plays a central role in supporting the development and promotion of standards. NIST’s 2019 plan entitled “US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools,” posits that “standards should be complemented by related tools to advance the development and adoption of effective, reliable, robust, and trustworthy AI technologies.” Collectively, this plan and NIST’s other recent work represent a useful blueprint for the federal government to follow in building effective standards that incorporate the insights of many different stakeholders and that are likely to be adopted voluntarily by industry, minimizing the need for explicit and onerous regulations. Putting NIST’s Plan at the center of efforts to build AI trustworthiness standards would also align with the direction Congress has signaled through recent legislation to focus on the development of AI standards, which authorizes several AI standards programs at NIST. Policymakers should consider taking the following steps to accelerate the establishment of standards for trustworthy AI:

• Congress should provide sufficient appropriations to NIST to execute its existing AI standards activities and new activities authorized by the National Artificial Intelligence Initiative Act of 2020. Funding can help ensure that NIST can accomplish its own fundamental R&D activities, in conjunction with industry, to support the development of standards while positioning the United States to be a global leader in AI standards development among its partner nations.

• NIST should expeditiously implement its programs authorized by National Artificial Intelligence Initiative Act of 2020 and develop a timeline on key AI standards activities to provide transparency to stakeholders and Congress.
Expansion of access to government data sets to train AI models

Federal, state, and local government agencies maintain large and relevant data sets that can be of tremendous value to developing innovative and trustworthy AI applications. Identified as a priority by 61 percent of respondents, these data sets can be valuable due to improved training of AI models and the mitigation of biases stemming from insufficiently diverse sources of data. For example, government data sets often include anonymized data relating to large cross-sections of the American population, a larger and more diverse group of individuals than the customer or user base of many commercial products. For example, government data sets may also integrate writing samples and spoken language examples from numerous linguistic, ethnic, and socioeconomic groups, enabling systems that depend on interpretation of natural language to be tested across a very wide range of inputs.47

Overall, the federal government should develop and support shared data models and public data sets, following the approach taken by the OPEN Government Data Act to ensure that government data sets are of high quality and made available in structured, widely used, and machine-readable formats. To effectively leverage government datasets and models for AI, policymakers should consider the following recommendations:

• Congress and federal agencies should ensure that appropriate funding is made available, and captured in annual budget requests, to support the implementation of the OPEN Government Data Act and for the continued improvements of quality and accessibility of federal government data.

• Federal agencies should work to encourage both state and local governments to share their data sets on a voluntary basis, and in coordination with any existing standards and with respect to any applicable law. This collaboration can enrich federal data sets and identify resource needs by state and local governments, such as technical expertise and funding, to execute this objective.

• The federal government should explore creating a pilot program to enable the voluntary sharing of private sector data to address pressing national challenges and bolster existing government data sets to improve the quality and usability of the data. The pilot program should be voluntary and should consider methods to encourage private sector participation.

• The federal government should also consider publication of non-sensitive and unclassified AI models to act as patterns on which further improvements and innovations might be built by the private sector.
Encourage sharing computing resources to advance AI

The development of AI applications often requires significant computing resources that some in academia and in the private sector do not possess. Enabling shared resources for AI research and development can spur the development of new technologies by giving both government agencies, private-sector startups, and academia the tools they need to rapidly prototype and test novel and innovative AI applications. Identified as a priority by 42 percent of respondents, public computational resources for training AI models could expand access to AI research similar to the way that the National Science Foundation’s Computer Science Network expansion of the early ARPANET to academia expanded participation in networking that would eventually lead to the commercial Internet. Specifically, government agencies should aim to enable collaboration on core computational resources including:

- Implement Section 5106 of the Fiscal Year 2021 National Defense Authorization Act, the National AI Research Resource Task Force, which creates a task force of industry, academia, and government to develop a roadmap and implementation plan to create a national shared computing resource for AI.
- Support investments in hardware, optimized software, and computational strategies, leveraging partnerships with private sector leaders, to increase the efficiency and performance of the research cloud, as a strategy to maintain global leadership in computational aspects of AI. These activities should be conducted in coordination with any other relevant plans and programs.
- Create interactive curricula and sandbox training environments to support students and early-stage professionals in developing the skills to build high-performing AI applications, including the shared computing resources needed to train AI models.

Establish interoperability standards for edge AI hardware and devices

As use cases such as visual inspection, sound and vibration analysis, and automated vehicles become a more significant part of the economy, more attention should be paid to edge AI hardware and software. Edge hardware and software enable AI models to run locally on devices to improve speed of decision-making and faster response times and protect data privacy by filtering sensitive data before it is stored or crosses the network. Identified as a priority by 50 percent of respondents, interoperability standards for edge AI hardware and devices can enable more efficient design of complex systems of edge AI devices, as well as providing common standards for testing the reliability of devices and securing them from new types of threats. Key policy recommendations to help enable edge AI includes:

- Support for interoperability standards for edge AI devices, through the expansion and codification of existing collaborations between the private sector, enabling new innovators to contribute to an expanding ecosystem by providing additional capabilities to existing configurations.
- Establishment of leading practices for securing edge AI devices, which due to their wide distribution can be more difficult to monitor and more vulnerable to physical manipulation or intrusion.
Support the creation of open-source tools and frameworks

Collaboration between government, academia, and the private sector can be a critical aspect of the development of AI innovations in the United States. Identified as a priority by 54 percent of respondents, open-source tools and frameworks can be used for designing and training AI data models and for assessing and mitigating issues of AI trustworthiness. Improved access to AI development through the use of open-source development tools and frameworks further expands the range of participants involved in the AI innovation ecosystem. Also, open-source tools and frameworks can help ensure that the insights and leading practices into trustworthy AI practices and techniques are shared widely within the AI stakeholder community. To better leverage open-source tools and frameworks, policymakers should consider several policy solutions:

• Encourage federal agencies to develop standard operating procedures to facilitate the publishing of open-source software as an output of their internal trustworthy AI development efforts, including models, tools, and training data sets, to enable reuse of government-developed resources to accelerate academic and commercial projects, except in cases where such publication would compromise national security or other confidential information.

• Expedi-tiously implement an AI Risk Management Framework, as required by Section 5301(c) of the Fiscal Year 2021 National Defense Authorization Act. The risk management framework is a voluntary, consensus-based process intended to mitigate risks throughout the development and deployment of an AI system through developing common definitions of key AI terms, create guidelines and best practices, and provide case studies to effectively implement the framework.

Enfranchising the American workforce in AI innovation

Ensuring that American workers are full participants in the AI economy of the future is likely a crucial issue for the long-term maintenance of American leadership in AI. The United States should look to have the broadest possible segment of its workforce to have the necessary skills to engage in AI-enabled industries and occupations. This can also help ensure that workers and the public can trust that AI applications will augment existing jobs and create new job opportunities rather than eliminate jobs. The federal government, in collaboration with employers and mindful labor market trends, should support the successful transition of the American workforce into a future AI-enabled economy by:

• Funding employer-led reskilling and retraining programs that emphasize AI literacy and support workers in finding roles that complement AI systems, or in using them productively to augment existing skills.

• Providing resources to assist state and local governments in modernizing K-12 and higher education in partnership with the private sector, to include more opportunities for students to interact with, train, and develop AI models, helping enable a seamless transition into a professional life where AI is ubiquitous.

• Promoting resources including financing tools, that enable lifelong learning and continuing education to help ensure that even the workforce’s newest members can continue to evolve their skills in a world of continuous technological change.
Building and supporting international partnerships in the adoption of trustworthy AI worldwide and to counter digital protectionism

Ninety-five percent of consumers worldwide are located outside the United States. American companies therefore should access foreign markets to grow their businesses and remain globally competitive. Governments around the world, including China, the European Union, and India, are increasingly turning to protectionist measures to discriminate against US companies with new taxes and regulations that diminish US market access, and steal American intellectual property. The rise of digital protectionism, which is well catalogued in the US Trade Representative’s annual *National Trade Estimate*, directly and negatively effects American competitiveness in artificial intelligence. Strategies to counter these measures by negotiating high-standard digital trade commitments with new trading partners and vigorously enforcing existing trade obligations where they are violated may be needed.

Interoperable frameworks for operating across markets also can make it easier for companies to ensure compliance with the widest possible range of regulatory environments while minimizing market-specific adjustments to the design and operation of their products and services. Thus, it can be in the interest of the United States to maintain continuous communication with its trading partners on the evolving definition of trustworthy AI and to help establish interoperable frameworks for the governance of AI technologies.

The Department of State, the Department of Commerce, the US Trade Representative, as well as regulatory authorities, all play important roles in ensuring that foreign governments do not create barriers to trade in AI technologies or to services enabled by AI technologies; favor their own domestic AI technologies unfairly; or establish permanent bans or unreasonably high regulations relating to the use of specific AI technologies or techniques.

There are a number of international partnerships around AI trustworthiness that can be leveraged by the United States for global cooperation on AI. Some of these include:

- **The Global Partnership on Artificial Intelligence (GPAI),** was launched in June 2020 as “a mechanism for sharing multidisciplinary research and identifying key issues among AI practitioners, with the objective of facilitating international collaboration, reducing duplication, acting as a global reference point for specific AI issues, and ultimately promoting trust in and the adoption of trustworthy AI.” This organization enacts a key principle of the Organization for Economic Cooperation and Development’s (OECD) Recommendation on Artificial Intelligence to “provide a forum for exchanging information on AI policy and activities.”

- **Existing bodies for the study and dissemination of information related to trustworthy AI sponsored by the OECD, including the OECD AI Policy Observatory (OECD AI).**
In addition, high-standard digital trade agreements, which may be needed to counter the growth of digital protectionism more broadly, are increasingly incorporating specific commitments on trustworthy artificial intelligence. The Digital Economy Partnership Agreement, signed by Singapore, New Zealand, and Chile, as well the Australia-Singapore Digital Economy Agreement include first-of-their kind disciplines on artificial intelligence. These commitments complement high-standard protections for algorithms and source code included in the US-Mexico-Canada Agreement and the US-Japan Digital Trade Agreement.

By taking a proactive role in the establishment of thoughtful guidelines for trustworthy AI in international standards-setting bodies, global initiatives, and trade organizations, the federal government, in partnership with industry leaders can establish leadership and encourage consensus around solutions that mitigate risks while enabling innovation. Specifically, the federal government should consider taking the following steps to champion trustworthy AI policies internationally:

- Negotiate international trade agreements that incorporate high-standard commitments on the digital economy, including in bilateral, regional, and plurilateral settings. These agreements should continue to incorporate protections that are foundational to the use and development of AI in global markets. The US Trade Representative, in consultation with the business community and other stakeholders across the federal government should consider whether new trade disciplines specifically devoted to AI may be needed.

- Proactively and regularly engage with US trading partners on matters of AI governance. As recognized in the OMB’s AI regulatory guidance, regulatory agencies should engage with their foreign counterparts to promote consistent regulatory approaches to AI that promote compatible regulatory approaches to AI and to promote AI innovation. These dialogues serve as valuable opportunities to share leading practices, data, and lessons learned, and help ensure that the US remains at the forefront of AI development. Importantly, international regulatory engagement can minimize the risk of unnecessary regulatory divergences from risk-based approaches implemented by US trading partners. US engagement on international AI governance should extend to multilateral and regional forums, including the OECD, GPAI, and APEC, among international institutions. Consider advancing important standards policy in support of open and competitive markets, particularly with emerging technology initiatives. The development of global standards in collaboration with the private sector is likely the best way to promote common approaches that are technically sound to deliver on technology solutions and policy objectives. Such standards should be voluntary, open, transparent, globally recognized, consensus-based, and technology-neutral. On AI technical standards, the federal government should consider the following actions to exercise leadership internationally: 1) Create a strategy to demonstrate global leadership in and support initiatives to develop AI standards; 2) Play a convening role with the private sector to help ensure appropriate industry representation at standards-setting bodies and organizations; and 3) Promote the use and broad adoption of standards developed by non-government organizations.
CASE STUDY 1

Driving trustworthy AI through research and development investments

Overview of AI research and development investments

An important function of the federal government in supporting innovation is providing federal investments towards R&D. Federal investments will likely be needed to remain competitive with the increased R&D investments of other nations. Overall R&D expenditures in the United States, both public and private, have not risen significantly, as a share of GDP, since 1996. As the Bipartisan Policy Center notes, in the same time period, China increased its R&D expense four-fold, while countries like Israel and South Korea also significantly ramped up spending. The result is that the United States’ share of global R&D has declined over the past several decades, falling from 69 percent in 1960 to 28 percent in 2016. From 2000 to 2015, the United States accounted for 19 percent of global R&D growth, while China accounted for 31 percent, and in purchasing power parity-adjusted dollars, China has already outpaced the United States in total R&D investment. Expansion of federal AI R&D capacity can be accomplished through increasing investments in existing programs as well as creation of new programs, especially for agencies such as the Department of Energy, the National Science Foundation, Department of Defense, and NIST. While the enacted FY2021 federal AI non-DoD R&D budget was $1.5 billion, a 34 percent increase over the FY2020 figures, many organizations have suggested this number should grow. In April 2020, the National Security Commission on Artificial Intelligence (NSCAI) recommended a doubling of non-DoD AI R&D funding to $2 billion, focusing on the value of fundamental research and particularly microelectronics technologies as crucial enablers of American competitiveness. The Bipartisan Policy Center has further recommended a continuing increase of total federal AI R&D spending to reach $25 billion by FY2025. To meet this objective, federal AI R&D investment would need to significantly grow year over year.
While government support can lower barriers for innovation and entrepreneurship, ultimately the market provides resources more efficiently to help enable companies to commercialize their technology.

To keep pace with the demand for AI innovation, the federal government should increase its investments in AI R&D and encourage partnerships with the private sector. A recent review by the Congressional Budget Office (CBO) highlights two basic themes about how government R&D investments translate into broader economic impacts. First, fundamental research takes approximately 20 years to manifest its full economic impact as it works its way from the laboratory to commercial products. Second, federal R&D spending is more valuable to the overall economy when directed toward early-stage technology development, as private interests have incentives to focus on development of technologies closer to the stage of commercialization and are less likely to incubate promising research that has not yet shown commercial potential. Overall, government involvement in early development of critical technologies can have numerous benefits: fundamental research serves as the foundation of new innovations, accelerates the growth and maturation of these technologies, and reduces barriers to entry for startups and entrepreneurs to bring their novel insights to market.

Survey results on AI research and development

Respondents to the survey strongly supported expansion of the AI R&D capacity of the federal government, with over 70 percent of respondents recommending prioritization of this area. Respondents also agreed that the federal government should invest more in research and development of AI technologies, with 43 percent supporting "much more" investment relative to other R&D priorities, and another 46 percent supporting "somewhat more" investment.

Relative to other priorities for R&D funding, should the government invest more, or invest less, in AI technologies in general?
Respondents to the survey were also asked to identify how their organization currently funds AI innovation to determine the opportunity for expanding government R&D partnerships with the private sector. 90 percent of respondents funded AI innovation in whole or in part with their own internal, organizational budget. 23 percent received some form of sole or supplemental investor funding, and 4 percent had identified other sources of funding such as donations or project-based revenue. Only 12 percent of respondents indicated that some or all of their AI innovation funding came from government sources.

Which of the following best represents how your organization funds new AI innovation?

Among the 88 percent of respondents who were not currently receiving funding for new AI innovation from the government, the majority expressed willingness to do so, with 64 percent indicating that they were either “extremely” or “slightly willing.” Only 10 percent expressed active uninterest, a relatively low number given the administrative requirements that can come with seeking or receiving government support. The high willingness on the part of organizations to receive government funding for innovation is likely a recognition that the challenges of developing trustworthy and reliable AI systems are large, and that many of the largest costs associated with AI innovation, such as building high quality data sets and training models appropriately, can effectively be achieved in partnership with public sector entities.

You previously indicated your organization does not currently receive funding for new AI innovation from the government. Which of the following best represents your organization’s willingness to receive government funding for AI?
Respondents to the survey strongly agreed that government investment was more important at the fundamental research stage and for early-stage startups, with 61 percent of respondents agreeing that government support was an important source of funding for fundamental research and 44 percent agreeing that government support was of benefit to early-stage startups. A diminishing number of respondents identified government funding as important to companies progressing through the stages of commercialization. While government support can lower barriers for innovation and entrepreneurship, ultimately the market provides resources more efficiently to help enable companies to commercialize their technology. This indicates that government should consider seeking connections with academic institutions, incubators, the venture arms of larger companies, and other organizations that foster new initiatives, rather than focusing partnerships commercializing products for the market.

Respondents to the survey were generally confident that government policies could in fact support the development of trustworthy AI applications, with 30 percent of respondents suggesting that government involvement could ensure trustworthy AI development to a “great extent” and an additional 53 percent of respondents agreeing that this involvement could ensure trustworthy AI development to at least “some extent.” Interviews with AI experts and industry leaders conducted during the development of the survey reinforced the idea that many researchers, entrepreneurs, and businesses involved in AI would welcome government investment in research, standards, and training data required to produce more trustworthy AI systems.

To what extent can government investment or intervention ensure that research and development in AI leads to innovation in trustworthy AI applications?

In your observation, across the wide range of companies that produce AI innovations, at which stage of development would government investment provide a significant source of funding?

![Graph showing responses to the question:](image)
Modeling the impact of increased government AI R&D

Assessing the total economic impact of federal R&D investments in AI typically requires extrapolation from previous examples where government intervention in an emerging technology sector provided a foundation for accelerated growth in the private sector. In recommending an overall investment of $40 billion in AI research and development, inclusive of both defense and non-defense R&D, the NSCAI report notes that the equivalent of $96 billion was put into the development of the Interstate Highway System in 1956. The implication is that the long-term economic and social transformations enabled by earlier investments that could potentially be exceeded by an investment not even half as large. While individual states had initially made great strides in linking local and regional centers with roads, the standardization and comprehensiveness of the Interstate Highway System made it possible for all parts of the country to benefit from increased access to raw materials and talent, in addition to providing a resilient infrastructure for national defense purposes. By 2011, the Department of Transportation attributed $15 trillion of economic activity to trucking and freight transportation enabled by the Interstate Highway System. This is an increase of over 150 times the original investment, or approximately 9.6 percent of annual compounded growth on the original investment over the 55-year period.

Also, a National Research Council study from 2001 discussed the $7 billion (1999 dollars) of investments of the Department of Energy in a range of energy efficiency and storage technologies over a 22-year period led to approximately $30 billion (1999 dollars) in the form of economic net benefits. These benefits include commercialization of energy-saving technologies and cost savings to businesses and consumers from increased energy efficiency, slightly more than a fourfold return on the original investment, or approximately 6.8 percent annual compounded growth over the 22-year period.

Taking these two examples indicate a broader pattern of return on government R&D investment, we can begin to establish a picture of the return on R&D investments that might occur if recommendations for increasing AI R&D investments were enacted. Extrapolating over a 20-year period, and assuming that return on AI is similar to the pattern seen in previous productivity-increasing transformations, the yield on the Bipartisan Policy Center’s total recommended federal AI R&D expenditure of $25 billion would result in between $94 billion and $156 billion of incremental economic impact by 2045. This assumes a low case of 6.8 percent compound annual return and a high case of 9.6 percent compound annual return per the historical examples.
Relative to previous technology revolutions, however, there is evidence that AI has a potentially higher total economic value than many previous technologies. A 2018 paper looking at the impacts of robotic automation technologies implemented between 1993 and 2007 determined that they contributed a net 0.36 percentage points of annual labor productivity to the economy.\(^{65}\) Also, a 2017 NBER paper compared the period after portable power became available in production (1890 to 1940) with the period of the uptake of information technology (1970 to 2017) and showed that both periods showed a similar trend in increasing contribution to productivity over time after a slower period of adjustment as the new technologies became integrated into business processes.\(^{66}\) A productivity-based approach to modeling economic impact was taken by an Analysis Group paper from 2016, which argued that if the overall effects of AI were similar in impact to that of the diffusion of mobile phone technology throughout the 1990s and 2000s, it would contribute between 0.31 and 0.43 percentage points of incremental GDP annually. If instead, AI had an even broader impact, equivalent to that of the widespread adoption of all forms of new information and communications technology throughout the same period, the economic impact would be equivalent to an incremental 0.8 percentage points of GDP.\(^{67}\)

Moreover, a 2019 European University Institute paper suggests that due to its capacity for self-improvement, AI should not be conceptualized simply as a new type of automation, but as a “completely new input of production,” potentially increasing not only labor productivity or return on capital investments but making entirely new tasks possible.\(^{68}\) This would imply that AI’s contribution to productivity could significantly exceed that of previous transformative technologies. Even if AI is taken to contribute only the equivalent of robotics or mobile telephones, this could represent over $477 billion in GDP growth through 2025. However, if AI is truly unlike previous generations of technologies and yields productivity improvements in excess of all previous information technology investments, with a 1.2-point contribution to productivity growth, the impact could be as great as $1.4 trillion of additional GDP through 2025.

Finally, the likelihood of achieving a higher outcome from AI R&D investments relative to previous transformative technologies could also be accelerated by the significant investments that the private sector is making in AI R&D. Private companies in the United States are expected to spend almost $100 billion annually on AI R&D by 2025.\(^{69}\) Though only a portion of overall increase in productivity from AI can be directly attributed to public R&D investments, making federal investments in AI R&D a significant priority to help facilitate the continued growth of an AI economy.

<table>
<thead>
<tr>
<th>Year</th>
<th>GDP Estimate</th>
<th>Low Case (0.4 points)</th>
<th>High Case (1.2 points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021</td>
<td>21,921.6</td>
<td>87.7</td>
<td>263.1</td>
</tr>
<tr>
<td>2022</td>
<td>22,967.7</td>
<td>91.9</td>
<td>275.6</td>
</tr>
<tr>
<td>2023</td>
<td>23,913.1</td>
<td>95.7</td>
<td>287.9</td>
</tr>
<tr>
<td>2024</td>
<td>24,833.8</td>
<td>99.3</td>
<td>298.0</td>
</tr>
<tr>
<td>2025</td>
<td>25,783.4</td>
<td>103.1</td>
<td>309.4</td>
</tr>
</tbody>
</table>

GDP estimates from October 2020 edition of IMF World Economic Outlook, all figures in US dollars in billions

The yield on the Bipartisan Policy Center’s total recommended federal AI R&D expenditure of $25 billion would result in between $94 billion and $156 billion of incremental economic impact by 2045.
Investing in trustworthy AI

The overall strategy for allocation of investment and prioritization of federal government AI research and development will require leadership from the White House Office of Science and Technology Policy in coordination with other federal agencies engaged in AI R&D activities given that AI crosses a number of different sectors and applications. Given the significant potential economic impact of AI innovation for the United States economy, the policymakers should prioritize investments in AI R&D through:

- Enacting the recommendations of the NSCAI final report, the Bipartisan Policy Center, and other organizations that suggest dramatically investing in AI R&D by the federal government.
- Fully appropriating programs established in the National Artificial Intelligence Initiative Act of 2020 at the National Science Foundation, Department of Energy, and the Department of Commerce that focus on AI R&D.
- Identifying new opportunities to bolster federal government investments in trustworthy AI R&D and that can contribute to AI-related research and create of pipeline of innovation that can be further developed and commercialized by the private sector.

Given the significant potential economic impact of AI innovation for the United States economy, the policymakers should prioritize investments in AI R&D.
CASE STUDY 2

Government modeling of trustworthy AI

The federal government should lead in trustworthy AI innovation from the front, acting as a role model for states, local governments, and the private sector in the responsible use and implementation of AI systems that serve citizens and conduct government business. Federal agencies are already putting AI-enabled solutions in place to improve government services. For example, in 2015, US Citizenship and Immigration Services (USCIS) had deployed a chatbot “Emma,” which fields over 14 million queries related to immigration issues each year.99 When asked about government interventions that were likely to support trustworthy AI innovations, 53 percent of respondents indicated that the government itself model the implementation of trustworthy AI systems. This finding was emphasized by the NSCAI's Final report, which noted that:

“Public trust will hinge on justified assurance that government use of AI will respect privacy, civil liberties, and civil rights. The government must earn that trust and ensure that its use of AI tools is effective, legitimate, and lawful. This imperative calls for developing AI tools to enhance oversight and auditing, increasing public transparency about AI use, and building AI systems that advance the goals of privacy preservation and fairness. It also requires ensuring that those impacted by government actions involving AI can seek redress and have due process.”

This case study takes a deeper dive into how the federal government can promote trustworthy AI through its own use of trustworthy AI applications, focusing on four different categories of policy solutions:

• Implementation of AI in e-government applications that serve citizens
• Implementation of AI in applications used internally by federal agencies
• Development of novel AI applications to address public crises
• Establishment of procurement processes for AI technologies that establish guidelines for trustworthiness
Survey respondents were asked how they would prioritize government engagement in modeling implementations of trustworthy AI systems. 73 percent of respondents indicated support for the development of novel AI applications to address public crises such as the pandemic or climate change. 71 percent of respondents also saw value in the establishment of procurement processes for AI technologies that incorporated guidelines around AI trustworthiness. There was also substantial support for the implementation of trustworthy AI in applications used internally by federal agencies (supported by 67 percent of respondents) and in e-government applications oriented toward citizens (supported by 61 percent of respondents).

Prioritization of these four areas can build public awareness of, and confidence in, the positive applications of AI. Many government systems today are widely used by the public and are some of the most important and influential points of interaction through which the public can understand and trust AI systems. Moreover, government modeling of AI applications can serve as an example for the private sector and other governments to encourage the use of trustworthy AI technologies. We will now examine each of these four areas in more depth and provide policy recommendations to help further government adoption of trustworthy AI applications.

Among the ways in which government can model implementation of trustworthy AI system, which of the following should the government prioritize?
Leverage AI to address national and global crises

To build trust in AI technologies, there may be no greater opportunity than the government advance of AI innovations that directly and publicly address the most consequential crises that pose a threat to our nation and our world. Some AI systems are able to predict and mitigate significant threats to human life and property from extreme events such as pandemics, and climate disruptions such as extreme weather events, and crippling disruptions of essential utilities and supply chains. Also, AI can be used to improve forecasting of extreme weather and provide earlier warning in cases of potential disasters, as well as model impacts of exceptional flooding, seawater intrusion, and other early indicators of sea-level rise. As the COVID-19 pandemic becomes more manageable in the United States through mass vaccinations and improved public health awareness, AI can be used to rapidly identify clusters of new cases or the spread of novel variants, enabling more targeted public health interventions that protect the economy while helping mitigate rapid increases in cases.70

While private sector partners can contribute insight and technology to these challenges, government has a unique role in driving development of novel applications in these spaces as a result of both its scale and its capacity to invest in long-term, transformational initiatives. To effectively leverage AI applications to help address national and global crises such as COVID-19 and climate change, policymakers should consider the following recommendations:

• Federal agencies should identify and prioritize the use of AI applications that could be used by government and by private sector and civil society stakeholders to address pressing public crises. Agencies should also identify any barriers that prevent or inhibit the development and use of identified AI tools.

• Federal agencies should sponsor public contests or prizes to encourage private citizens, academia, and the private sector to incentivize the development of novel, AI-driven solutions to address public crises.
Establish trustworthy AI procurement policies

The federal government is a major purchaser of information technology (IT) and services, spending $90 billion on IT annually. Federal government standards often become the de facto baseline for many vendors in designing security, privacy, compliance, and other features, and aligning private sector procurement policies with these standards can help mitigate risks and costs associated with noncompliance. As applied to AI, by building ethical guardrails based on the core principles of trustworthy AI into its procurement policies, the federal government can incentivize vendors into adopting trustworthy AI concepts in the design of their AI products and services. This can be analogous to Executive Order 13834, “Efficient Federal Operations” which encouraged suppliers to offer more eco-friendly and sustainable products. Moreover, these standards can even encourage consistency internationally just as the costs and complexity of complying with the EU’s General Data Protection Regulation drove many American companies to adopt GDPR obligations as a baseline for their domestic products and services even in the absence of equivalent legislation within the United States.

Policymakers can take several steps to position the United States government as a leader in trustworthy AI through procurement:

- Through the General Services Administration’s AI Center of Excellence, the federal government should conduct an assessment of how to integrate trustworthy AI principles in the procurement of AI technologies. The assessment should account for existing federal policies and guidelines, and ongoing efforts to define trustworthy AI, and should involve consultation with external stakeholders, including industry.

- The federal government should publish its procurement standards, best practices, and other processes for use, on a voluntary basis by the private sector and subnational governments to inform the development of their own processes to adopt trustworthy AI technologies.
Implement AI technologies in internal and external federal agency applications

Executive Order 13859, “Maintaining American Leadership in Artificial Intelligence” emphasized the importance for federal agencies to adopt AI technologies in their own operations, noting that agencies applying for purposes such as regulatory compliance, combatting waste, fraud and abuse, identifying and mitigating cybersecurity threats, among many other uses. Facilitating progress in AI adoption across federal agencies has been a priority of the General Services Administration (GSA), which established an Artificial Intelligence Center of Excellence within its Technology Transformation Services (TTS) division in 2017 to accelerate the use of AI as part of IT modernization initiatives within federal agencies. Krista Kinnard, Director of the Artificial Intelligence Center of Excellence, describes four key areas where federal agencies are already seeing success in the adoption of AI technologies:

“Broadly, we see a lot that focus on four outcomes: increased speed and efficiency, cost avoidance and cost saving, improved response time, and increased quality and compliance... One of the biggest areas we’ve started to see advancement is in data management. Agencies are using intelligent systems to automate both collection and aggregation of government data, as well as provide deeper understanding and more targeted analysis. We have seen that the potential for the use of natural language processing (NLP) is huge in government... So much of government data exists in government forms with open text fields and government documents, like memos and policy documents. NLP can really help to understand the relationships between these data and provide deeper insight for government decision making.” —Forbes

Ultimately, federal agencies should leverage their growing expertise in AI to extend a greater range of AI capabilities to citizens through e-government applications and other agency applications. Accelerating decision-making and simplification of processes enabled by AI technologies can reduce the time and effort associated with common tasks undertaken by the public such as filing taxes, applying for licenses and certificates, and engaging in the development of public policies. The improved experience of government services enabled by AI can build citizen trust both in AI technologies and in the functions of government itself. Policymakers should take the following steps to implement AI applications in the federal government:

- Fully implement the AI in Government Act, including the timely development of guidance for federal agency use of AI applications and the codification of the AI Center of Excellence.
- Federal agencies should issue a request for information to gather private sector input to identify how cutting-edge AI applications can assist federal agencies in their public-facing responsibilities.
Conclusion

The United States has an enormous opportunity to transform its economy and society in positive ways through leading in AI innovation. While AI technologies can pose risks, appropriate policies, as outlined in this paper, can help mitigate and address those risks, which could help increase public trust in AI. Moreover, the numerous benefits of AI also will likely improve AI trustworthiness among the public, which can be accelerated through public policy solutions. Guiding AI innovation in accordance with trustworthy AI can ultimately encourage the social and economic benefits derived from AI and empower the United States to maintain global competitiveness in this critical technology sector. The federal government should support the development of trustworthy AI through common-sense policies that foster growth and innovation while ensuring that new technologies are deployed responsibly. A dynamic future of human-centered AI innovation is available to us, one that can encourage economic growth and social development within the United States and across the world.

A dynamic future of human-centered AI innovation is available to us, one that can encourage economic growth and social development within the United States and across the world.
Appendix

Survey methodology

The recommendations and results in this paper are supported by a survey of 250 respondents involved in AI research and development or decision-making by companies based in or operating primarily in the United States. These respondents came from a wide cross-section of industries, with 32 percent in the IT or telecommunications sectors, 20 percent from industrial sectors including automotive, electronic equipment and instruments, semiconductor, aerospace and defense, and other manufacturing verticals, 11 percent from the healthcare and pharmaceuticals sector, 10 percent from financial services firms, 8 percent from business or professional services firms, 6 percent from the retail sector, 4 percent from the energy sector, 4 percent from the media and entertainment sector, and 5 percent from other sectors of the economy. 46 percent of respondents came from companies with over $1B+ in annual revenue, 29 percent from companies between $100M and $1B in annual revenue, and 25 percent from companies with less than $100M in annual revenue or undisclosed revenue.

Respondents were generally senior, with 44 percent in C-level or equivalent roles, 21 percent in SVP or VP roles, 28 percent in director or manager roles, and 7 percent working as individual contributors or in other roles. 70 percent held an IT- or technology-related role in their company, 28 percent came from research and development groups, and 2 percent came from human resources roles, segments targeted by the survey because of their likely exposure to AI technologies and their impacts. The complete survey results are located in the appendix of this paper.
Survey respondent population

In which of the following countries does your organization operate?

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>13%</td>
</tr>
<tr>
<td>Germany</td>
<td>16%</td>
</tr>
<tr>
<td>US</td>
<td>100%</td>
</tr>
<tr>
<td>Italy</td>
<td>11%</td>
</tr>
<tr>
<td>Spain</td>
<td>12%</td>
</tr>
<tr>
<td>UK</td>
<td>20%</td>
</tr>
<tr>
<td>Others</td>
<td>7%</td>
</tr>
</tbody>
</table>

Which of the following most accurately reflects your industry?

- Financial Services: 10%
- Automotive: 2%
- Telecommunications: 3%
- Electronic Equipment and Instruments: 2%
- Semiconductor Technologies: 2%
- Healthcare/Pharmaceuticals: 11%
- Media/Entertainment: 4%
- Aerospace & Defense: 4%
- Information Technology Service: 29%
- Manufacturing: 10%
- Retail: 0%
- Business/Professional Services: 8%
- Others: 5%

What was your organization’s approximate total revenue in the last fiscal year?

- Less than $100M: 20%
- $100M - $499M: 12%
- $500M - $999M: 16%
- $1B - $2B: 13%
- $2.1B - $5B: 19%
- More than $5B: 15%
- Unsure/cannot discuss: 19%

Which of the following best describes your department within your organization?

- Human Resources: 28%
- IT/Data and Information: 70%
- Research & Development: 2%

Which best describes your title?

- C-level or equivalent: 44%
- VP-level or equivalent: 11%
- Director-level or equivalent: 10%
- Manager-level or equivalent: 8%
- Individual contributor: 6%
- SWP-level or equivalent: 5%
- Others: 0.8%
About the authors

Kate Schmidt
Kate Schmidt is COO for the Global Deloitte AI Institute. Kate focuses on amplifying Deloitte’s Age of With™ messaging in the market, and connecting Deloitte’s clients to the AI ecosystem. Prior to her role within the Deloitte AI Institute, Kate led large scale global finance transformation programs in consumer and industrial products, life sciences, and high tech industries.

Matt Furlow
Matt Furlow serves as a Policy Director at the U.S. Chamber of Commerce Technology Engagement Center (C_TEC). He leads the portfolio on emerging technology issues primarily focusing on innovative transportation technologies and automation. Prior to the Chamber, Furlow was a Legislative Director for a member of Congress focusing on transportation and defense issues.
About the Deloitte AI Institute
The Deloitte AI Institute helps organizations connect all the different dimensions of the robust, highly dynamic and rapidly evolving AI ecosystem. The AI Institute leads conversations on applied AI innovation across industries, with cutting-edge insights, to promote human-machine collaboration in the “Age of With”.

Deloitte AI Institute aims to promote the dialogue and development of artificial intelligence, stimulate innovation, and examine challenges to AI implementation and ways to address them. The AI Institute collaborates with an ecosystem composed of academic research groups, start-ups, entrepreneurs, innovators, mature AI product leaders, and AI visionaries, to explore key areas of artificial intelligence including risks, policies, ethics, future of work and talent, and applied AI use cases. Combined with Deloitte’s deep knowledge and experience in artificial intelligence applications, the Institute helps make sense of this complex ecosystem, and as a result, deliver impactful perspectives to help organizations succeed by making informed AI decisions.

No matter what stage of the AI journey you’re in; whether you’re a board member or a C-Suite leader driving strategy for your organization, or a hands on data scientist, bringing an AI strategy to life, the Deloitte AI institute can help you learn more about how enterprises across the world are leveraging AI for a competitive advantage. Visit us at the Deloitte AI Institute for a full body of our work, subscribe to our podcasts and newsletter, and join us at our meet ups and live events. Let’s explore the future of AI together.

www.deloitte.com/us/AIIInstitute

About the Chamber Technology Engagement Center
Our nation’s future economic success, growth, and competitiveness depends on a thriving and innovative technology sector. Every company is a tech company and data-driven innovation is the foundation of businesses across the country. The Chamber Technology Engagement Center (C_TEC) tells the story of technology’s role in our economy and advocates for rational policy solutions that drive economic growth, spur innovation, and create jobs.

The U.S. Chamber of Commerce is the world’s largest business organization representing companies of all sizes across every sector of the economy. Our members range from the small businesses and local chambers of commerce that line the Main Streets of America to leading industry associations and large corporations.

They all share one thing: They count on the U.S. Chamber to be their voice in Washington, across the country, and around the world. For more than 100 years, we have advocated for pro-business policies that help businesses create jobs and grow our economy.

www.americaninnovators.com
www.uschamber.com
Endnotes


21. **These American workers are the most afraid of A.I. taking their jobs**, CNBC, November 7, 2019.


28. **Holon IQ, February 2020.**

29. **Holon IQ, February 2020.**


32. **These American workers are the most afraid of A.I. taking their jobs**, CNBC, November 7, 2019.


43. **Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government Executive Office of the President, December 8, 2020.**


46. **Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation, October 28, 2019, accessed via Center for Security and Emerging Technology, Georgetown University Walsh School of Foreign Service, June 22, 2021.**

68. The Economics of Artificial Intelligence: A Survey, European University Institute, Robert Schuman Center for Advanced Studies, July 2019.
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0207
Comment on FR Doc # 2023 12995

Submitter Information

Email: [redacted]
Organization: Knowing Machines Research Group

General Comment

See attached file(s)

Attachments

Knowing Machines_OSTP Worker Surveillance Comment
The Knowing Machines Research Group (Knowing Machines) submits these comments in response to White House Office of Science and Technology Policy’s (OSTP) May 3, 2023 Request for Information on Automated Worker Surveillance and Management (RFI).\textsuperscript{4} In alignment with its 2022 Blueprint for an AI Bill of Rights, OSTP is considering the “prevalence, impacts, and deployment” of worker surveillance technologies and how Federal agencies can help “ensure that these systems do not undermine workers’ rights or their safety.”\textsuperscript{5} The OSTP is considering a wide range of impacts on workers, including their “physical and mental health; privacy; dignity, and autonomy; and ability to exercise workplace rights.”\textsuperscript{6}

We appreciate the opportunity to contribute to OSTP’s inquiry. Knowing Machines is an interdisciplinary research project tracing the histories, practices, and politics of how automated systems are trained to interpret the world from vast, nebulous datasets. Our research targets the assumptions underlying emerging machine-learning technologies with the hope that greater transparency will encourage meaningful interventions.\textsuperscript{7} We are a team of lawyers, computer scientists, science and technology studies (STS) professors, artists, and data scientists who have

\begin{footnotesize}
\begin{itemize}
    \item \textsuperscript{1} Legal Research Fellow, The Knowing Machines Research Project; Supervising Attorney, NYU’s Technology Law & Policy Clinic, and Fellow, Engelberg Center on Innovation Law & Policy, NYU School of Law.
    \item \textsuperscript{2} Lead Principal Investigator, The Knowing Machines Research Project; Research Professor of Communication and STS, USC Annenberg School for Communication and Journalism; Senior Principal Researcher, Microsoft Research Lab (NYC).
    \item \textsuperscript{3} Co-Principal Investigator, The Knowing Machines Research Project; Professor of Clinical Law, Director of NYU’s Technology Law & Policy Clinic, and Co-Director of the Engelberg Center on Innovation Law & Policy, NYU School of Law.
    \item \textsuperscript{4} 88 Fed Reg. 27,932, available at https://www.federalregister.gov/documents/2023/05/03/2023-09353/request-for-information-automated-worker-surveillance-and-management.
    \item \textsuperscript{5} Id. at 27,934.
    \item \textsuperscript{6} Id.
    \item \textsuperscript{7} For more information, see https://knowingmachines.org.
\end{itemize}
\end{footnotesize}
published extensively on the techniques and harms of automated surveillance technologies, including in the workplace—whether that be the factory floor, warehouse, office, or the home.⁸

Knowing Machines urges OSTP to translate workers’ expectations of privacy in their data into guidance for employers on when and what types of data they can collect. As worker data fuels automated surveillance technologies by serving as training data for machine-learning models, we encourage OSTP to set a high bar for employers who exploit worker data to inform employment decision and undermine workers’ autonomy. Specifically, we propose OSTP collaborate with other federal agencies to set baseline protections over worker data that align with the limits on health data for healthcare providers and on consumer financial data for financial institutions respectively. At a minimum, we hope OSTP will adopt clear policies protecting worker data relating to union organizing communications and activities.

1. Automated Worker Surveillance and Management Systems Depend on Massive Amounts of Worker Data

The pandemic and its aftermath have intensified existing rifts over worker autonomy and control in the U.S.⁹ Especially as young adults enter a workforce shaped by decades-long wage stagnation, anemic unionization, and regular waves of mass layoffs, they are proving immune to the promises of “workism”—the belief that “work is not only necessary to economic production, but also the centerpiece of one’s identity and life’s purpose.”¹⁰ Attention-grabbing buzzwords like “the Great Resignation”, “quiet quitting”, and the “anti-work movement” attempt to capture a

---


⁹ See Limitless Worker Surveillance, supra note 8, at 111–13 (describing the changing nature of work in the U.S., including pre-pandemic increases in remote workers and freelance workers).

broader sense of turmoil in our relationship to work, boundaries, and living a meaningful life both in and beyond our jobs.\textsuperscript{11}

Yet workism persists, with around 40\% of workers seeing their jobs as central to their overall identities regardless of gender, race, ethnicity, or age.\textsuperscript{12} While certain groups of workers—educated young men, high-earners, and recovering workaholics—are spending less time working than pre-pandemic,\textsuperscript{13} employers continue to project their “productivity paranoia” onto workers of all stripes.\textsuperscript{14} This has led to a sharp increase in surveillance technologies permeating the average workday. Searches for employee monitoring software increased by 75\% in March 2020 compared with the 2019 monthly average, and now around 80\% of employers use monitoring software to track employee performance and online activity.\textsuperscript{15}

Today, technology is a critical factor in both what we do for work and how we do it. But while employers have been rapidly adopting new methods of AI-driven automated worker surveillance,\textsuperscript{16} this phenomenon is a continuation of much older labor practices established in the late nineteenth and early twentieth centuries.\textsuperscript{17} As one of us has previously noted, “[w]e are witnessing new refrains on an old theme.”\textsuperscript{18} The atomized, tedious work of early factories

\begin{footnotes}
\textsuperscript{16} In this Response, we focus on machine learning-based technologies of worker surveillance. We use the term “AI”, aware of its misleading anthropomorphism, to refer to technical systems that rely on machine learning models trained on datasets to extract patterns and use those patterns to predict outcomes in new contexts. See generally Sarah Clston, \textit{A Critical Field Guide for Working with Machine Learning Datasets} (2023), https://knowingmachines.org/critical-field-guide.
\textsuperscript{17} See ATLAS of AI, supra note 8, at 59 (“[The encroachment of] AI into the workplace should properly be understood as a return to older practices of industrial labor exploitation that were well established in the 1890s and the early twentieth century.”); Saima Akhtar, \textit{Employers’ New Tools To Surveil and Monitor Workers Are Historically Rooted}, Wash. Post (May 6, 2021), https://www.washingtonpost.com/outlook/2021/05/06/employers-new-tools-surveil-monitor-workers-are-historically-rooted/ (“The history of worker surveillance shows that today’s cutting-edge time-tracking technologies are just new iterations of an old industrial technique—only now, these technologies are more discreet and pervasive.”). For a robust historical analysis of worker surveillance in the U.S., see Ifeoma Ajunwa, \textit{The Quantified Worker: Law and Technology in the Modern Workplace} 179–87 (2023).
\textsuperscript{18} ATLAS of AI, supra note 8, at 29.
\end{footnotes}
required managers to maintain efficient and disciplined workers. This necessitated new systems of observation and control for managers that drew from earlier systems, including the 1780s’ inspection house that placed all of a factory’s workers within constant sight of their supervisors, and the central role of overseers for slave owners in the plantation colonies of the Americas. This historic oversight role has been “primarily deputized to surveillance technologies” today. But what these technologies enable is a more granular and invasive degree of worker surveillance than historical human managers could ever dream of.

There are several types of automated worker surveillance. Much of it is deployed to placate the employer that workers are really working. This includes activity monitoring, or surveilling how workers spend their time through tools that “track[] idle time, record[] keystrokes, or even periodically screenshot[] an employee’s computer.” But there are also several types of surveillance that go beyond monitoring productivity to uncover workers’ personal behaviors and characteristics. So-called “bossware” programs that monitor and collect data from workers’ emails, telephones, and online activities can be used to gauge productivity, but that data can also reveal personal behaviors and characteristics with no connection to one’s work. Other examples include location tracking, video camera surveillance, measuring workers’ use of different applications on digital devices, and even biometric surveillance tools that use facial recognition to ensure that workers remain in front of their computer screens during business hours. Behavioral surveillance tools not only measure productivity and compliance with company policies, but some also attempt to predict when workers might be likely to quit. And tools like emotion recognition analysis are used to gauge a job candidate’s “fit” with the

---

19 See id. at 60–61.
20 Id. at 61–63.
21 Id. at 62.
22 Akhtar, supra note 17 ("Although the surveillance and punishment of 'wasted time' on the factory floor has remained fairly consistent over the past century, the way workers' time gets tracked and recorded has become more invasive due to advancements in technology.").
23 A full survey is outside of the scope of this Response but can be found in various publications. See, e.g., Ajunwa, supra note 17, at 187–92 (2023) (providing an overview of modern worker surveillance); Limitless Worker Surveillance, supra note 8, at 108–113 (gathering similar examples).
24 Ajunwa, supra note 17, at 189.
26 See Ajunwa, supra note 17, at 190–91.
27 Id. at 191.
prospective employer, based on pseudoscientific conclusions about the ways we express emotions through facial gestures alone.\textsuperscript{28} Sometimes, data collected from costumers—like their traffic patterns and other interactions with products and employees—lead to indirect worker surveillance, informing employers how many workers to schedule and where.\textsuperscript{29}

These technologies inform the field of “people analytics” built on the vast digital data generated mostly passively as workers perform their daily activities.\textsuperscript{30} Its central premise is that as much data must be collected as possible, so that these data can provide accurate insights into persistent managerial questions, including who to hire or promote, who is likely to leave, who has been working collaboratively despite working remotely, and whether workers feel fulfilled professionally.\textsuperscript{31} The algorithms that interpret these data are increasingly used to inform employment decisions, whether or not workers are aware of the surveillance.\textsuperscript{32}

People analytics beget an intimately quantified modern worker.\textsuperscript{33} Whereas Taylorist theories of management focused on mastering a single task along the assembly line and maximizing production efficiency, people analytics has shifted focus onto the individual worker as a cite of self-mastery to save the employer time and money.\textsuperscript{34} Surveillance technologies allow employers to be omnipresent in each of their workers’ lives without physically being anywhere near them, enabling uninterrupted monitoring of a person’s communications, movements, and activities even outside of work.\textsuperscript{35} Employers have converted their workers into “captive audiences for data extraction,” using these technologies to indiscriminately capture and transfer worker data that is

\textsuperscript{29} Ajunwa, supra note 17, at 174.
\textsuperscript{30} See Jeffrey T. Polzer, The Rise of People Analytics and the Future of Organizational Research, 42 ORGANIZATIONAL BEHAV. 1 (2023), https://www.bbe.edu/rie/Publication%20Files/1-s2.0-S0191308523000011-main_0230d385-13af4a01-9b68-c6b07be05ce2.pdf.
\textsuperscript{31} Id. at 174.
\textsuperscript{32} Id. at 3 (“Workers are being quantified as never before as the ongoing digital revolution converts every action and interaction into a trail of data. These data can be fed into algorithm, which can then produce predictions, categorizations, and suggestions to change behavior.”). See also Alex Christian, The Employee Surveillance that Fuels Worker Distrust, BBC (June 27, 2022), https://www.bbc.com/worklife/article/20220621-the-employee-surveillance-that-fuels-worker-distrust (“Often, this [bossware] technology runs undetected, meaning workers can be unaware that their boss is effectively spying on them.”).
\textsuperscript{33} See generally Ajunwa, supra note 17.
\textsuperscript{34} Limitless Worker Surveillance, supra note 8, at 137.
\textsuperscript{35} Id. at 138; see also Ajunwa, supra note 17, at 175 (“Surveillance technologies are what has enabled management to become less visible, yet more powerful.”).
often personal and sensitive.36 For our colleague and worker surveillance expert Ifeoma Ajunwa, this data is “captured capital” as it “is siphoned from workers both knowingly and unknowingly as part of the employment bargain.”37 Workers have no uniform privacy protections to this data,38 and they largely lack any bargaining power over how employers exploit their data.39

There is a direct link between the exploitation of worker data and automated worker surveillance. Put simply, “[d]ata obtained through employee surveillance fuels AI.”40 As worker data becomes more legible and sortable into distinct categories, it can be used to train machine-learning models that undergird AI technologies used to interpret worker behavior. This creates a dangerous cycle: workers use technologies that produce data, that data is compiled into vast datasets, those datasets are used to train models, those models influence algorithms to find certain associations in the data, and then those algorithms power automated surveillance tools used by employers to decide whether workers are being sufficiently productive, loyal, and compliant. Pairing the “voracious maw of data collection” with the “inexplicability of decisions made” from automated systems leads to workers feeling “trapped in a matrix of computer-controlled reality from which there is no escape.”41

There is growing concern about the misuse of data to train machine-learning models powering automated surveillance technologies, and worker data should be no exception.42 In its consideration of automated worker surveillance systems, OSTP must be mindful of the enclosure of worker data that enables the development of these systems in the first place. The lack of clear privacy protections for worker data provides OSTP a unique opportunity to guide employers on when and what types of worker data they can collect, store, use, and sell. OSTP must act now to

36 Ajunwa, supra note 17, at 178.
37 Id. at 177.
38 Limitless Worker Surveillance, supra note 8, at 113–28 (analyzing extant legal protections and their weaknesses).
39 See Atlas of AI, supra note 8, at 58 (“The terms [of AI in the workplace] are based on a significant power asymmetry—is there ever a choice not to collaborate with algorithmic systems? When a company introduces a new AI platform, workers are rarely allowed to opt out.”); Kate Crawford, Amazon’s Union Vote Could Be a Harbinger for the Future of Work, WASH. POST (Apr. 10, 2021) (“Artificial intelligence systems are increasingly used to track, assess, and rank workers—often without their knowledge. This, in turn, acts as a force multiplier for the asymmetries of power between bosses and employees.”); Pauline T. Kim & Matthew T. Bodie, Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy, 35 ABA J. LABOR & EMP. L. 289, 292 (2021), https://www.americanbar.org/content/dam/aba/publications/aba_journal_of_labor_employment_law/v35/no-2/artificial-intelligence.pdf (“Employees report a feeling of powerlessness when AI is given significant power over their jobs, as they lose the ability to interact with their ‘supervisor’ in a meaningful way.”).
40 Kim & Bodie, supra note 39, at 301.
41 Id. at 292.
counterbalance employers’ insatiable thirst for more comprehensive and invasive worker data to fuel people analytics solutions, bringing autonomy over worker data explicitly into the conversation.

II. OSTP Should Adopt Baseline Worker Data Privacy Guidance to Deter Unchecked Worker Surveillance by Employers

In its Blueprint for an AI Bill of Rights, OSTP recognized that individuals and their communities “should be free from unchecked surveillance; surveillance technologies should be subject to heightened oversight.”23 Responding to Question 5. of the RFI, Knowing Machines encourages OSTP to develop guidance for employers who currently deploy automated worker surveillance systems or are considering doing so.24 We are mindful that often specific statutes and regulations governing security, access, and notice and consent regimes “provide insufficient guidance for decisions about the reuse and repurposing of information when companies can manipulate huge amounts of data” collected through worker surveillance.25 Instead, we agree that “broader principles have to be developed that can guide privacy decisions consistently in a variety of contexts,” and those broader principles should draw from workers’ own expectations about their data “as a touchstone for developing [employers’] privacy practices, including the [employer’s] definition of privacy.”26 Beyond simply punishing bad behavior, federal agencies beginning with OSTP must encourage employer responsibility for protecting worker privacy.27

Because automated worker surveillance technologies require vast amounts of worker data for training purposes, employers are currently incentivized to collect worker data with abandon. OSTP should consider adopting guidance that proposes internal guardrails for employers over when and what types of worker data they are able to collect and process. To this end, we suggest OSTP help disincentive limitless worker surveillance by encouraging employers to treat worker

---

24 In particular, Knowing Machines responds to 5.c., which asks “What policies or actions should Federal agencies consider to protect workers’ rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?” 88 Fed Reg. at 27936.
26 Id. at 64, 65.
27 See id. at 246.
data with the same level of care that healthcare providers treat health data and financial institutions treat consumer financial data. This guidance should be informed first and foremost by workers' own expectations of privacy over their communications, locations, behaviors, and other forms of personal data, especially where employers cannot show that these data and work performance are connected or such connections are attenuated at best.

Furthermore, we encourage OSTP to explore numerous worker data protections that will impact the viability of automated surveillance technologies driven by AI today. First, OSTP should work with other agencies to develop data privacy requirements in vendor agreements for automated surveillance products, including strict data minimization procedures and use limitation requirements to ensure that only the necessary amount of data is collected for a specific employment use (ideally limited to human resources and diversity initiatives), and data collected in one context is not later applied in employment decisions in other contexts. For companies that collect worker data into databases that could be used to train automated technologies, OSTP can incentive greater clarity around database access and licensing by requiring employers to appoint dataset stewards who can decide and document how datasets may be used, derived from, and distributed outside of the employer.

Additionally, OSTP can work with organized and organizing workers fighting back against automated worker surveillance to protect them from employer interference and retaliation. In line with recent decision by the National Labor Relations Board against Amazon’s anti-union surveillance efforts, OSTP can adopt clear policies prohibiting the collection of worker data

---

50 See Ajunwa, supra note 17, at 202 (discussing how, when state law does not specifically prohibit worker surveillance, courts weigh an employer's need to conduct surveillance against the employee's reasonable expectation of privacy); Ifeoma Ajunwa, Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, 63 St. Louis U. L.J. 21, 49 (2018), https://scholarship.law.shu.edu/jl/vol63/iss1/4/ (“While a reasonable expectation of privacy is well defined for Fourth Amendment cases, it is not as defined within the employment context, and some scholars have argued that workplaces operate as ‘private governments’ with employers exercising near dictatorial power over what privacy rights may be granted to workers.”).
51 See Feng, Mathur & Narayan, supra note 42, at 9–10 (describing how dataset creators should best steward datasets to minimize downstream misuses of the underlying data).
related to organizing and union participation.\textsuperscript{52} By protecting workers from the weaponization of their data to thwart organizing efforts, OSTP will enable workers to collectively bargain with their employers about the specific, context-dependent limitations they seek over their own workplace surveillance and their employers’ access to their personal data.\textsuperscript{53}

III. Conclusion

Knowing Machines supports OSTP’s critical inquiry into the massive reach of automated worker surveillance technologies and their negative impacts on workers’ lives. OSTP should develop guidance on baseline privacy protections that mediate the inherent power differential between employers and workers over control of their data. We encourage OSTP to emphasize the centrality of worker data to automated surveillance technologies powered by AI, as worker data informs the training of models that then influence algorithmic decision-making in opaque and unjust ways. If OSTP has any further questions, please reach out to Legal Research Fellow Melodi Dincer at [email protected] or Co-Principal Investigator Jason Schultz at [email protected]

Respectfully Submitted,

(b) (6)

Melodi Dincer  
Legal Research Fellow  
Knowing Machines Research Group


\textsuperscript{53} See Hearing from the American People: How Are Automated Tools Being Used To Surveil, Monitor, and Manage Workers?, WHITE HOUSE OFFICE SCI. & TECH. POL’Y (May 1, 2023), https://www.whitehouse.gov/ostp/news-updates/2023/05/01/hearing-from-the-american-people-how-are-automated-tools-being-used-to-surveil-monitor-and-manage-workers/ (“Monitoring conversations can deter workers from exercising their rights to organize and collectively bargain with their employers.”).
Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0208
Comment on FR Doc # 2023 12995

Submitter Information

Email: [REDACTED]
Organization: TechEquity Collaborative

General Comment

In the Matter of Request for Information: Automated Worker Surveillance and Management, Docket No. OSTP FRDOC 0001 0004 comments submitted by TechEquity Collaborative (attached)

Attachments

WH RFI on Automated Management filed by TechEquity Collaborative on 6.24.23
Before the
White House Office of Science and Technology Policy

In the Matter of:
Request for Information: Automated Worker Surveillance and Management

Docket No. OSTP FRDOC 000 0004

Comments of
TechEquity Collaborative

Samantha Gordon
Chief Program Officer
TechEquity Collaborative

Filed on June 24, 2023
Re: Comment on Workplace Surveillance and Automated Management

TechEquity Collaborative respectfully submits the following comment in response to the White House and Office of Science and Technology Policy (OSTP) Request for Information on Workplace Surveillance and Automated Management in May of 2023. We are appreciative of the White House and OSTP’s attention to these issues and their impact on workers’ rights.

Our comments will center on the experience of contract workers in the technology industry. We believe that these workers and all contracted and gig workers are at a particular risk for harm in automated management and workplace surveillance systems due to the precarious and fissured relationship between contract workers and their employers.

Our comments reflect the first hand experiences shared with our organization as part of our Contract Worker Disparity Project, they include:

- Importance of centering contract workers’ experiences in designing interventions on workplace surveillance and automated management
- Current harms contract workers in tech are experiencing as a result of automated management and fissured workplace structures
- Proposed policy and regulatory interventions, specific to automated management and workplace surveillance, based on the experiences of contract workers we have interviewed and surveyed

Additionally, we have submitted our name to comments that were developed by the Center for Democracy and Technology (CDT) which detail the impact of these tools on workers’ rights to health and safety, organize, non discrimination, and fair compensation.

Background and Definitions

Background

TechEquity Collaborative: Who We Are
At TechEquity Collaborative, we envision a world where the growth of the tech industry creates economic prosperity for everyone, and where tech sector employees and companies are engaged and active participants in making our economy equitable. Our mission is to mobilize tech workers and companies to advance structural change that addresses economic inequity at its roots. We educate the tech community on economic justice, advocate for bold public policy, and develop equitable corporate practices that build equity and opportunity in the broader economy. We run a series of initiatives that are focused on addressing inequities within the tech industry and inequities that result from tech’s products and business models.

You can find more information about us at https://techequitycollaborative.org/about/.

**Contract Worker Disparity Project**

In 202 , we launched the Contract Worker Disparity Project that investigates how an entire class of tech workers has been locked out of tech’s prosperity. We interviewed 30 contract workers one on one to learn about their experiences and conducted a survey of over 800 contract workers the largest of its kind in the tech industry. Additionally, we developed four white papers documenting why companies use contractors, where this phenomenon originates from, who often takes these jobs, and what it means for the tech industry.

In 2022, we published a final report of our research findings, outlining that temporary, contract, and contingent workers, who are hired through contracting agencies, are often doing the same work as their directly employed peers while making less money, receiving fewer benefits, and experiencing career immobility. Additionally, our research found that these workers were disproportionately Black, brown, indigenous, women, and non-binary as compared to their directly employed counterparts. We issued a Responsible Contracting Standard with specific guidance to support companies who want to ensure that they are creating resilient and healthy workplaces for their entire workforce. We passed first in the nation legislation in California to address a core problem in the contract work ecosystem lack of data and transparency.

**Definitions**

1. Con rac Worker D spar y Projec (n d) Con rac Worker D spar y Projec Re r eved June 9 2023 rom h ps://con rac work echequ yco abora ve org/ 2 Con rac Worker D spar y Projec 2022 Repor (n d) ech qu y Co abora ve Re r eved June 9 2023 rom h ps://ech equ yco abora ve org/down oad he con rac worker d spar y projec 2022 repor / 3 ech qu y (2022 Oc ober 5) Pay r ansparency s aw n Ca om a ech qu yCo abora ve h ps://ech equ yco abora ve org/2022/ 0/05/pay r ansparency s aw n ca om a/
Electronic Surveillance and Automated Management (ESAM)

As outlined in several memos directed to federal agencies, the Center for Democracy and Technology, and others, have defined Electronic Surveillance and Automated Management (ESAM) as follows:

- **ESAM consists of techniques to remotely manage workforces, relying on data collection and surveillance of workers to enable automated or semi-automated decisions.**
  - There are several categories of workplace surveillance technologies, including: remote monitoring and tracking, gamification, and algorithmic management.
    - Remote monitoring and time tracking allows companies to enforce pace of work policies that may not even be known to workers.
    - Gamification describes technology that is meant to motivate workers “using video game elements, such as digital points, badges, and friendly competition.”
    - Algorithmic management is the overarching system that takes input from these surveillance technologies and makes assessments sometimes leading to disciplinary action and adjustments to increase worker productivity.
- **The types of technologies that enable ESAM include: handheld devices, point of sale systems, mobile phones, fingerprint scanners, fitness and wellness apps, cameras, microphones, body sensors, keycards, electronic communication monitoring, geolocation tracking, collaboration tools, and customer review solicitation.**

A thorough database of these types of tools has been developed by Coworker.org as part of their Bossware and Employment Tech Database. Additionally, the University of California at Berkeley Labor Center compiled a report on the types of tools that are being utilized or developed and their potential for worker harm.

Contract Worker, Contracted Tech Worker, and Contracting Agencies

For brevity we’ve chosen some key words to refer to the contracting world. When we say contract workers we are referring to any worker who is hired through a third party (vendor, staffing agency, or payroll company) but who performs their day to day work for a tech company. This group includes a wide ranging set of workers from service workers (like janitors and security officers) to technical workers (like software engineers). When we say contracting agencies we are including hiring agencies, staffing agencies, payroll agencies, and vendors.

---

Fissured workplace

A concept that was articulated by David Weil in his book, The Fissured Workplace, a fissured workplace describes the outcome of the growing scale of domestic and global outsourcing. The basic concept was well summarized by reviewer Mike Konczal: “the result of corporations increasingly distributing activities through an extensive network of contracting, outsourcing, franchising, and ownership. Workers are less likely to work for the corporation that ultimately profits from their labor; instead, they work for a loose network of middlemen or as independent contractors. Their work is still monitored and controlled as closely as any other office worker, but they lose the protections of labor law and the ability to fully enjoy the rewards of economic growth. This is the new reality for workers in the 21st century.”

Importance of Including Workers in Fissured and Precarious Work Environments in ESAM Interventions

There are a variety of well documented cases of ESAM’s use and impact on vulnerable populations. Our particular focus for this comment is on the experiences of contract workers within the tech industry. Our research has shown that these workers are disproportionately women, non-binary, and people of color as compared to the directly employed tech workforce. Additionally, we believe that fissured work structures heighten the opportunity for worker harm and help employers avoid accountability. Our comments center on the experiences of these workers because this is our area of expertise.

I. Understanding Tech’s Reliance on Third Party Contract Workforce

Tech has long been lauded as a great industry for workers providing high salaries, generous benefits, equity and stock options, and a host of fringe perks like massages, free food, and more. As the tech industry enters a new stage with new challenges, we’ve seen those famously shiny tech jobs start to look less appealing with the industry conducting wide ranging layoffs, standing up massive lobbying operations to fend off regulatory efforts, and advocates are raising
questions about the resiliency of their commitment to expanding equity and inclusion. Throughout these challenges, one dynamic has stayed consistent – tech’s use of a shadow workforce to do some of the most psychologically damaging and mission critical pieces of work in the industry. However, many of these workers – the temporary, contract, and contingent workers who are classified differently from their directly employed counterparts – have been locked out of tech’s prosperity.

To better understand contracted tech workers’ experiences, we interviewed over 30 current and former contract workers, and ran a survey with 800 respondents, with both qualitative and quantitative responses. Across sources and surveys, certain findings are consistent: 

- **Contract workers of color are more likely to be paid hourly than annually, and to receive lower pay than white workers:** 39% of contractors of color are paid annually, compared to 45% of white contractors with the majority of contractors of color earning in the $50 85K range, compared to the majority of white contractors earning in the $85 20K range.
- **Contract workers of color are less likely to be converted to direct employment than white contract workers:** 4% of respondents who were people of color said they never converted to direct employment compared to 3% of white respondents.
- **Contract workers receive fewer benefits than direct tech workers:** 33% of survey respondents received no benefits, compared to just 23% of private industry workers who do not have paid vacation or sick leave.
- **People of color are overrepresented in contract roles compared to the overall tech workforce:** 44% of contractors are people of color vs. 3% in the direct workforce.

II. Recognizing the Dangerous Conditions and Potential for Discrimination in Contract and Temp Work Across all Industries is Critical

This phenomenon is not unique to the tech industry. Research conducted by workers rights’ advocates in Illinois found that staffing agencies employing temp workers exhibited a dramatic pattern of racial discrimination in their placements. Additionally, this research found that Black
and Latino workers comprise 85% of blue collar temp assignments in Chicago but only account for 40% of the population. 4

Not only is temporary and contingent work paid less often for performing similar jobs and overrepresented by people of color, it can be very dangerous work. Temp work has been documented as a safety risk for workers for nearly a decade. From a ProPublica investigation in 2015: [an] analysis of millions of workers’ compensation claims shows that in five states, representing more than a fifth of the U.S. population, temps face a significantly greater risk of getting injured on the job than permanent employees. In California and Florida, two of the largest states, temps had about 50 percent greater risk of being injured on the job than non temps. 15

In 2003, the Occupational Health and Safety Administration developed a Temp Worker Initiative due to several reports of fatalities of temp workers often on their first day of the job. 6 Since then, advocates have fought for greater protections for temp workers on the state level, including increased safety measures within the temp industry. 7

Despite its harms, the prevalence and scale of contingent employment has grown steadily over the past several years, outpacing direct employment at major companies like Google, which in March 2009 employed 20,000 contract workers and 02,000 direct employees. 8 As tech enters a cycle of layoffs, there are already indications that the use of temp work which increased dramatically after the 2008 financial crisis will increase as companies try to keep their productivity high and their official headcount low. 9 Since 2009, the ratio of contractors perhttp://www.chicagorunen.com/business/ctemp-agence...
employee has increased by more than 60%. More than half of all businesses with more than 25 employees use contractors.

**Current harms contract workers in tech are experiencing as a result of ESAM and fissured workplace structures**

Despite facing little regulation in the workplace, ESAM is contributing to the erosion of workers’ rights. In 202, we conducted 30 one on one interviews with 30 contract workers performing work for a tech company. Additionally, we surveyed 800 contract workers in tech. As a result of those interviews and survey responses, as well as a review of the relevant literature, we identified patterns that are outlined in a series of white papers and a summary report we published in 2022. In many of the interviews, workers highlighted the ways in which automated and algorithmic management systems were being deployed to evaluate their work, determine their pay, and influence their ability to be promoted or be terminated.

Below are the patterns we saw in those experiences. Where possible, we’ve included specific, first hand stories or quotes from workers. Our interviews were conducted with express consent from each worker that outlined that we may share their experiences in order to bring awareness to this issue and advocate for change, but we may not identify the worker themselves or attribute the quotes to them or their companies. Their names and employers have been removed, additionally we have anonymized identifiable information when a worker was describing specific responsibilities or tasks within their job, to ensure that they cannot be identified and do not face retaliation or retribution for sharing their experiences.

**ESAM erodes compensation and may lead to potential wage and hour violations**

ESAM systems are being utilized to evaluate work products and in some instances determine pay for contract workers in tech. In repeated interviews, we heard workers share similar patterns where they worked for a tech company, through a third party employer, and their work product

---

20 Sm a ek J mber S & Raff K (202 0) Compan es oard ng Work ers Cou d Be Good News or he New y ork mes h ps ///www ny mes com 202 0 / bs ness/economy/compan es hoard ng work ers h m
2 W ke (202 November 29) Con rac Work ers Grow ng As he U S Work once Grapp es W h abor Cons ra n s ( W ke d ) [Rev ew o Con rac Work ers Grow ng As he U S Work once Grapp es W h abor Cons ra n s] Gus o com Gus o h ps ///gus o com/company news/us con rac work 2022 survey
was often reviewed and assessed by an algorithmic or automated process. In some instances, that automated process denied workers pay, deemed their work product insufficient or low quality, and created a quota system for work production based on unknown information that was often unsustainable for workers.

One worker shared that when they submitted their work product for review, it would get rejected repeatedly. When asked what the rejection was based on they said that often the system provided a vague response such as ‘something went wrong’. The worker had to submit their work product through a third party application. They were transcribing and training an artificial intelligence system. To submit their work, they had to submit individual files one by one. In order to document that they had submitted these files, for their own records, they had to take individual screenshots of each submission on their phone or computer. Generally there were approximately 600 individual files for each hour of work. To self document their submission, would result in additional unpaid time for their labor. However, the worker was always torn about whether or not to take the time to do this and save it each time, for each hour of work, because when their work product was not recorded as having been submitted, they were not paid for their work. This worker was not an independent contractor, but a W2 employee of a third party contracting agency. They shared that when they submitted and the system would reject it or not recognize the submission, they would not get paid for that hour of work.

*Interviewer: When you were denied pay for your submitted work product, would the system say you were denied 1 of the submissions out of the hundreds you sent in? Or all of them?*  
*Worker: It will be that all 500 “weren’t submitted” so approximately a full 50 minutes of work that I then won’t get paid for. Even though I’ve completed the work.*  
*Interviewer: What can you do when it says that?*  
*Worker: Do it again.*

Workers shared that the standards around pay and employment are shifting due to the deployment of automated management systems. Many recounted that despite being a W2 employee of a contracting agency, they were only being paid for the hours they worked on a specific task, not the time they were clocked in and available to take a task or waiting for a task to be sent to them. Some shared that while this was the structure and their understanding, there were enough tasks that they did not have a lot of unpaid waiting time. However, the pay structures that many workers outlined may be in conflict with existing labor laws. We believe that the use of ESAM and lack of transparency create opaque and unclear standards that could result
in violations of the Fair Labor Standards Act and/or California’s labor code including wage and hour laws, standards for piece rate, standby time, and reporting to work time.\textsuperscript{22}

An additional experience that was shared by workers, outlined the way that ESAM systems were being deployed to surveil and compare workers productivity rates and contest whether or not a worker had completed an “appropriate” amount of work for the time they are said to have worked. These comparisons would theoretically lead to a reduction in pay or potential discipline. However, the workers shared that they had no way to verify if the comparison was accurate, what the employer deemed was an appropriate productivity rate or baseline, or whether or not there was a standard at which their pay would be reduced or they would be disciplined.

\textbf{Worker:} “They do track our ratings per hour. They use one person’s ratings per hour and compare it to other workers to determine if you billed the ‘correct amount of hours’ for that time period. For instance if the co-worker average was 200 tasks/hour but I billed at 150 tasks/hour, I would get an email warning me about an imbalance between the tasks I completed and the hours I billed for that work. We are tracked and there are these unseen expectations in our tracking and productivity rates.”

\textbf{ESAM systems lack transparency, feedback, or recourse for workers when they face discipline or contract termination}

Workers in fissured workplaces, like contract workers in the tech industry, experience difficulty in navigating workplaces with multiple employers—often they face opaque systems for feedback and performance management, an inability to access critical tools and training for their role, confusion over how to report workplace issues or discuss pay and promotions, and often workers report that they lack clarity on when or how their contract will be renewed, extended, or ended. When ESAM systems are introduced to the fissured workplace, these difficult structures become more intractable and can drive workers’ isolation and decrease their agency and ability to self-advocate.

In workplaces where ESAM systems were governing performance management, transparency and feedback became non-existent. Workers reported that they were completely unaware of what criteria their work was being evaluated on, often jumping through hoops and trying to reverse engineer outcomes from the ESAM system to determine what they may have done right or wrong in their work performance. Others reported that their requests for help or feedback...
often went into a digital void and they were unclear if they would ever get a response and had no other way to contact their employer for feedback.

The lack of clarity also impacted contract workers’ ability to take on work. From one interview with a contract worker:

**Worker:** “We have our commitments to complete every week but [because we haven’t been trained or know our criteria for quality work] we have to decide if it’s worth putting out potentially bad [training] data or not working.”

Another contract worker shared what it’s like to work with an ESAM system evaluating your work product and determining your performance:

**Worker:** “We are totally in the dark about how the data [we develop] is used. We can infer, but we don’t know. We just keep getting tasks, again and again, something pops up [telling you it’s wrong or being done incorrectly] and you wonder if you’re doing something wrong? But you don’t know why.”

**Interviewer:** Can you get feedback on what is going wrong or what you can do to improve?

**Worker:** Management says that they don’t know or can’t get the information. They tell us to just wait for 45 minutes and get another task sent to us.

**Interviewer:** What does it mean for you to not get this type of feedback?

**Worker:** If your data isn’t what they are looking for, you can be fired but you don’t have management or anyone telling you what’s wrong with the data.

When we interviewed workers about the feedback process, we heard various reports but when ESAM was implemented in the workplace, most feedback practices fit into two patterns either they can send a request for feedback to a digital system (an email, an app, etc.) or they can watch training videos to learn how to do the task. Below are some of the experiences that contract workers shared about the experience of getting feedback when ESAM is being utilized to evaluate their work product or performance.

“There is a generic email address we can send things to. We may get an answer back in three days or we may never get an answer.”

“At [redacted large tech company] we receive zero feedback. There are some tasks that give you feedback but it’s only when a task is being introduced to you [not once you start submitting the actual work product].”
“You might get a pop up that says you got this one wrong and this is how you should do it. The pop ups can be really helpful because in general you get no help at all, no one on one direction or feedback or any feedback whatsoever. It’s generally just an automated system.”

“You can look at your worker statistics and it will tell you how many were a blind/known answer you got wrong and how many you got right. This is the only idea you can get of how well you are doing.”

“I would really rather have more training and guidance than being fired if you don’t pass a blind test.”

**ESAM’s use in fissured workplaces creates another hurdle that chills worker voice and can lead to further erosion of job quality**

In our research on contract workers in the tech industry, we found that the precarious nature of a fissured workplace chilled worker voice. Because there are very few parameters for contract renewal and most are not visible to the workers themselves but instead are terms between the tech company and the contracting agency workers do not know how or why a contract will or will not be renewed. As a result, workers expressed that they are afraid to speak up against workplace harassment or other concerns for fear that their contract won’t be renewed. Additionally, workers do not want to be deemed “difficult to work with” as this impedes their potential for contract extension or transition to direct employment. Like most of these issues, the implementation of ESAM makes this existing precarity more extreme.

In workplaces with ESAM, contract workers reported that they had very few communication channels with other workers and experienced difficulty trying to build a peer network for feedback and troubleshooting on projects. Some contract workers reported that there was no way to know how many other workers were on the same project or what they were doing. Others shared that there was a place where you could see people working on your same project, but couldn’t communicate with them outside of exchanging information about that specific project. Many reported that their only means of communication with other workers was through company channels and was limited within those parameters. While communication with co workers and project managers is only a part of a worker’s experience we believe that these tools and channels are critical to worker satisfaction and job quality. Ensuring that workers can communicate with their peers can help them identify opportunities to strengthen their performance, share feedback, build worker voice, and improve workplace conditions.
An additional consequence of ESAM is the ways in which these systems can be used to degrade job quality over time. One contract worker shared their experience which captures this phenomenon.

“In my role as a contractor, I worked for the same staffing agency in three different capacities. Always that staffing agency and the only client was [redacted large tech company]. I was a full time employee for that staffing agency…I was paid by the hour. It was a minimum wage job. Then we got laid off and the [large tech company] wasn’t sending tasks. [The staffing agency] got back in touch a few months later. They asked us to do the same type of work. It was the same staffing agency but they were asking us to register on a freelance website like Upwork or Guru [to do the same job that would now be paid as piece work].”

ESAM has the ability to atomize work and workers themselves by disconnecting them from their peers, relegating feedback and job security to a pop up box, eroding workers’ compensation, and incentivizing employers to further degrade job quality.

**ESAM in the workplace must be regulated, and in some cases banned, by the federal government**

The imbalance of power between workers and employers makes the regulation of ESAM urgent and critical. Already there are many stories of growing worker surveillance, concerns around the growth of discriminatory hiring, and the emergence of algorithms to determine who gets laid off during a recession. Due to the spread of ESAM into many facets of work robust regulations and enforcement must be enacted and aggressively enforced to ensure that worker power is not further degraded in this moment of emerging technologies.

In 2022, we joined a coalition of labor unions and social justice organizations in California that introduced the Workplace Technology Accountability Act (AB 65 Asm. Kalra) to the California
legislature. AB 65 outlined a set of policies and parameters to govern the use of ESAM in the workplace, including: workers’ data rights, accountability in electronic monitoring, use of algorithms, requirement of impact assessments, and enforcement. From a letter to the Assembly Privacy and Consumer Protection Committee, bill supporters outlined that:

“We believe that employers can and should use digital technologies in the workplace in ways that benefit both workers and their businesses, and the goal of this bill is not to stop the use of technology or to block innovation. In fact, our members can offer many examples where technology has helped make jobs safer, opened up new skills and careers, and improved the quality of products and services. But it will take the type of robust standards and guardrails established in this bill to ensure that workers are not harmed by what is a rapidly evolving set of often unproven and untested technologies, many of which employers and even engineers themselves do not fully understand. By considering this bill, the California State Legislature has the opportunity to lead the U.S. in establishing workers as key constituents in decisions about how best to govern and oversee artificial intelligence and related technological innovations.

Policy interventions on ESAM that would benefit contract workers and all workers must include:

- Allow only for the collection of worker data that is strictly necessary for workers to do their jobs or for a valid business purpose.
- Ban unproven or high risk technologies like facial recognition and algorithms to predict worker behaviors unrelated to their jobs.
- Ban the use of ESAM only determinations for pay, promotions, discipline, or layoffs
- Require employers to notify workers about all relevant data collection, electronic monitoring, and algorithms in the workplace, prior to their use.
- Require employers to explain how these systems can affect employment decisions, including their assessment of workers’ performance or productivity.
- Allow workers to access and correct their data.
- Require pre deployment and periodic review to assess for discriminatory impact; utilizing a heightened set of standards for use in the workplace.
- Require employers to submit impact assessments to relevant government agencies.
• Require proactive and inclusive engagement of impacted people in the design, deployment, and enforcement of regulations of ESAMs.\textsuperscript{28}

• Create a public Registry of ESAM systems being deployed at private and public sector workplaces that includes the ability to search for algorithmic impact assessments;\textsuperscript{29} as well as any pending or completed investigations of complaints and the outcome, similar to databases that catalog consumer protection violations.\textsuperscript{30}

We believe that community and worker centered efforts like the Workplace Technology Accountability Act provide a pathway forward for policy intervention. Policies designed to support workers who will be impacted by the emergence and proliferation of ESAM must be developed with proactive, inclusive, and robust engagement of workers themselves. We appreciate the White House and OSTP for understanding the importance of public and worker engagement in the development of ESAM interventions and urge a continued effort to keep those communities engaged in the design, deployment, and monitoring of these interventions.

\textsuperscript{28}G\textsuperscript{erman} M \textsuperscript{n} (2022 November 2) Beyond Window Dressing Public Participation or Marginalized Communities. \texttt{papers.ssrn.com/ps/labs?abs=4266250}

\textsuperscript{29}\texttt{en-US} \texttt{Danish} (2020 June) The Use of Excellence in Usability Testing. \texttt{accessnow.org}

\textsuperscript{30}\texttt{Consumer} \texttt{Governed} \texttt{and Public Expenditure} (n.d) Consumer Nance and Public Research. \texttt{consumer.gov/daa-research/consumer-compa-n-s/}
PUBLIC SUBMISSION

Docket: OSTP TECH 2023 0004
Request for Information; Automated Worker Surveillance and Management

Comment On: OSTP TECH 2023 0004 0002
Request for Information: Extension of Comment Deadline Automated Worker Surveillance and Management

Document: OSTP-TECH-2023-0004-DRAFT-0209
Comment on FR Doc # 2023 12995

Submitter Information

Email: 
Organization: PowerSwitch Action, Chicago Gig Alliance/The People's Lobby, Colorado Independent Drivers United-CWA, Gig Workers Rising

General Comment

See attached file(s)

Attachments

6.23.23_OSTP_CommentLtr_Coalition
Comment submitted electronically via https://www.regulations.gov

June 23, 2023

Alan Mislove
Assistant Director for Data and Democracy
Office of Science and Technology Policy (OSTP)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: Request for Information: Automated Worker Surveillance and Management,
Document ID OSTP-TECH-2023-0004-0001

To Whom It May Concern:

We write to offer public comment on the request for information published on May 2, 2023 (Document 2023-09353).¹ We, the undersigned organizations—PowerSwitch Action, the Chicago Gig Alliance/The People’s Lobby, Colorado Independent Drivers United-CWA, and Gig Workers Rising—are pleased to share insights from research, analysis and worker interviews from our work across the country with app-based drivers.² This submission contains responses to questions in Sections 1. Worker Organizations (1a, 1c, 1k); 4. Data and Evidence (4b, 4d, 4e, 4k), and 5. Policies Practices or Standards (5c). For questions or to request a follow-up dialogue, discussion, or event, please contact Mariah Montgomery, National Campaigns Director, at

Organization Representing Workers (such as a workers center)

Q1a: Describe the relevant job, employer, and industry.

¹ The information in this document is provided for informational purposes only and does not contain legal advice, legal opinions, or any other form of advice regarding any specific facts or circumstances.

² In this document “app-based corporations” describes Uber, Lyft, and other businesses such as DoorDash and Grubhub, which provide rideshare or delivery services through a device-based application. “App-based driver” means someone who works for an app-based corporation to provide rides or deliveries on its platform.
Uber and Lyft emerged from the economic ashes of the global financial crisis in 2008. In a few short years, Uber, Lyft, and other app-based corporations became ubiquitous, with drivers and delivery workers in all 50 states. Researchers have highlighted that far from serving as a “fix” to the financial crisis, these corporations used widespread economic distress to organize vast numbers of unemployed workers, primarily people of color and immigrants, into a cheap, disposable workforce. By exploiting technology and devising aggressive expansion strategies to build substantial market power, app-based corporations sought to protect their business from market competition, strip drivers of their individual and associational rights, and dominate political decision-making. In so doing, they invented a whole new sector of distinctly dangerous jobs and corporations.

Despite portraying themselves as innovative and futuristic “disruptors” of modern industries, app-based corporations are taking advantage of automated surveillance and management technology to pursue the age-old corporate playbook of chasing profit at the expense of workers, worsening labor inequality. Scholars have described app-based drivers’ working conditions as a “‘worst of both worlds’” model, in which app-based corporations consider drivers to be self-employed, thus shifting nearly all operational costs and risks onto drivers, and yet exert a level of control that exceeds the standard employer/employee model.

Because the United States’ segregated economy leaves many Black, Latino, and immigrant workers with few other employment options, the app-based economy disproportionately employs workers of color. In a dynamic sociologist Tracie McMillan Cottom identifies as “predatory inclusion,” these workers are nominally included in app-based platforms that purport to offer opportunities for economic mobility, but instead procure labor on

---

7 As documented by the National Employment Law Project and others, in a period of four years, app-based corporations, primarily Uber and Lyft, adopted state interference—an antidemocratic practice favored by the gun and tobacco industries—to move state legislators in the vast majority of states to overrule and preempt local laws regulating their industry and to strip drivers of their rights. R. Smith et al., Uber State Interference, National Employment Law Project (Jan. 18, 2018), p. 4-5, https://tinyurl.com/mvwhsxnk.
9 Gebrial, supra note 5, p. 4.
10 Milner et al. supra note 8, p. 12.
fundamentally extractive terms. In a University of California study found that in Uber and Lyft’s hometown, San Francisco, 78% of app-based drivers are people of color, and 56% are immigrants. According to the same study, 71% of these app-based drivers work 30 hours a week, and more than half work over 40 hours a week. Despite this, more than one-fifth of drivers do not have health insurance, and 15% earn so little they rely on public assistance. Shockingly, as many as 20% of drivers may earn zero dollars after expenses.

In cities nationwide, drivers are organizing for respect on the job. On May 4, 2023, drivers from across the country—in Seattle, San Francisco, Los Angeles, Chicago, Denver, and New York—came together to demand improved safety, fair pay, and the end of unfair driver terminations. By shining a light on their dangerous and exploitative working conditions, drivers are demanding a fair return on the billions of dollars they make for these corporations.

Q1c: Describe the type of automated surveillance or management you have experienced, including the location of the monitoring technology

From the moment Uber and Lyft drivers log on to the app, they are subjected to constant digital surveillance. Drivers are expected to provide their own cell phone and car, to install the app on their personal devices, and submit to intensive identification and background checks. This provides Uber and Lyft with the opportunity to engage in intrusive surveillance and data extraction. App-based drivers have reported location tracking notifications while their apps were closed, high battery consumption, unusually high levels of data usage after giving the app permission to access their phone’s storage, and receiving notifications suggesting they log in while using a competing platform.

Once the app is installed, facial recognition technology in the phone camera monitors driver identification requirements. The app tracks drivers’ GPS location, speed, acceleration, and other data.

---

13 Ibid.
14 Ibid.
15 Ibid., p. 2–3.
18 Sannon, supra note 17, p. 6.
and hard stops. It monitors drivers’ acceptance, cancellation, and completion of passenger ride requests. It records driver and passenger in-app communications, as well as passengers’ ratings of each driver after the ride. The app instructs drivers which passengers to pick up where, what the driver’s estimated time of arrival is, and what directions a driver should follow to a passenger’s destination. If drivers deviate from these instructions, they risk discipline or, depending on the circumstances, even “deactivation” from the app.

Data from the app’s meticulous tracking of every aspect of the driver’s work is fed into an algorithm which makes the kind of decisions normally made by a human supervisor. The app determines which rides to allocate to which drivers, and how much to compensate drivers for those rides. Extracted data also continuously fine-tunes predictions about drivers’ future behaviors, which the app then uses to create individualized, gamified bonuses and other financial incentives to encourage workers to keep driving on the app’s desired terms. The algorithm uses this data, including passengers’ reviews, to compile data profiles of drivers. A recent Uber patent describes a “user profile store” for drivers, which stores information about “providers” (or drivers) which “may include type of service provided, provider ratings, data about past service, an average number of services per hour, vehicle type, common hours online, an average arrival time in relation to a predicted estimated time of arrival, whether the provider typically follows suggested service instructions (e.g., routes), geographical regions most frequently visited by the provider, an average amount of time the provider is willing to wait for a new assignment, and so forth.” The patent states that user profile data may be used to predict the likelihood of driver behavior, “for example, whether a provider is likely to follow a suggested service instruction, and whether a provider is likely to provide service among different geographical regions, for example, when responding to a service request from a requester [or passenger].”

---


22 Uber Privacy Notice, supra note 20, III.B.2; Lyft Privacy Policy, supra note 20, 2.B.


24 In this document, “deactivation” refers to when an app-based company blocks a worker’s access to the app either temporarily or permanently too often without warning or just cause. Essentially, deactivations are terminations or unpaid suspensions.


26 Vignola, supra note 21, p. 4; Mateescu, supra note 23, p. 5–6.

27 Ibid.


30 Ibid.
suspensions or deactivations from the app via electronic notification are not uncommon, and terminating drivers is highly dependent on data gathered through electronic surveillance.  

Drivers describe how the surface-level promise of efficient, error-free algorithmic management is belied by the reality of a clunky, unresponsive platform, which the driver is expected to “fix” on his or her own time. Simone, an Uber and Lyft driver in the San Francisco Bay Area, recalls a time when Uber failed to pay her for four rides, and the difficulties she encountered when contacting the company to resolve the issue. “You have to keep contacting them through the app – or you can call them. You’re on the phone with them for like 2 hours for any price adjustments.” As Simone states, “[T]hey don’t pay you for that. It’s a full-time job.” Some drivers are so discouraged that they stop contacting the company. Issa, an Uber and Lyft driver from Colorado who turned down a ride for safety reasons that was wrongfully counted towards her cancellation rate, explains: “I didn’t bother calling Uber to correct it. I didn’t want to spend the time. Lyft, you could never contact them. They are horrible. You can never get through to anyone.” A lack of transparency creates a lack of accountability.

Q1k. How automated surveillance and management has affected you—whether positively or negatively—including any economic, safety, physical, mental, and emotional impacts

Drivers we interviewed describe Uber’s and Lyft’s algorithmic payment systems as unjust and arbitrary. Certain drivers will ask passengers how much they are paying for a ride, only to discover it has no relationship to their compensation: “One time I know the passenger was paying $44 and after tolls I got $11.” Some drivers report that the companies’ individualized, variable pay rates for each ride seem to calculate the lowest amount of earnings a driver will accept. Ernesto, a driver for Uber and Lyft in Illinois observes that as he “drive[s] more or more

---

34 Id.
36 Uber and Lyft Driver (Anonymous, first name changed), supra note 33. See also Y. Zhou, Uber is hiding customer payments from drivers. Again, Mission Local (Nov. 16, 2022), https://tinyurl.com/v6z6h7k (reporting that on a sample of five rides booked by publication in San Francisco, drivers received less than half of what customers paid).
and more” he “make[s] less and less money.” Ernesto says, “The company doesn’t pay fairly. Somebody has to stop this company.”

Some drivers begin to see the various financial bonuses and incentives the app dangles in front of them as yet another form of manipulation, designed to make drivers spend longer periods of uncompensated time on the app waiting for a dispatched ride or bonus to supplement their otherwise meager, base-level earnings. Issa, a Colorado driver, describes what she calls the companies’ “algorithmic games,” like when “[y]ou are heading towards a bonus and they will send you on a long ride.” Issa reports that once when she was trying not to lose a consecutive ride bonus, the app sent her into the mountains in a snowstorm.” Inching along at 5 miles per hour, she managed to drop off her passenger, but on her way home, the roads were shut down, and she was stranded.

RJ, an Uber and Lyft driver from the San Francisco Bay Area, describes how the algorithmic “surge” pricing Uber offers—promising drivers higher pay if they relocate to specific places at specific times to give rides—can, at times, seem more like a form of “surge baiting,” in which no matter where the driver goes the surge line keeps moving, just out of reach. Describing the never-ending tug-of-war between the hope that the app will release a bonus, and the disappointment when it does not, John, an Uber and Lyft driver from Colorado, states, “Uber emotionally abused us.”

Drivers are so dependent on Uber and Lyft bonuses to supplement their scant baseline earnings that they sometimes feel compelled to accept rides, even in unsafe situations. Jasmine, an Uber driver in Illinois, recalls how one Saturday night, as she was working towards a bonus, she got a ride request from a passenger staying at a hotel, who was clearly using a fake name. Despite her intuition that it might be unsafe, she decided to pick up the passenger because the bonus was “critical to my earnings as a driver.” Jasmine experienced what she described as an attempted car-jacking when the passenger disclosed he was carrying a weapon, and another car started aggressively following her. Jasmine states: “As a driver, I rely on my instincts to keep

---

37 Uber and Lyft Driver (Anonymous, first name changed), phone interview by Avril Smith, Apr. 16, 2023. See also discussion infra note 141.
38 Id.
39 Uber and Lyft Driver (Anonymous, first name changed), supra note 35.
40 Id.
41 Id.
43 Id.
45 Id.
46 Id.
myself safe at work. However, … I don’t always get to follow my instincts because I also feel pressure to make money.”

Undergirding many drivers’ negative experiences with automated surveillance and management is their extreme vulnerability to the apps’ seemingly arbitrary and automatic deactivation of drivers. John reports the anxiety he experiences over the app’s constant tracking of his cancellation and passenger ratings, and the omnipresent threat of deactivation he feels if they dip too low. “Sometimes I want to cancel a ride because I know it’s a bad ride, but I accept it because I need to drive,” he shares. “The rating and customer canceling is a type of emotional abuse because we can’t defend ourselves and our numbers just go up and down.”

Adding to their sense of precarity, some drivers report that Uber and Lyft overwhelmingly deem passengers’ complaints about drivers as credible, while drivers’ complaints about passengers are not. As John states, “the [m]ajority of drivers are immigrants,” and “every time [customers] complain they deactivate them falsely.” Jasmine relates driving in a climate of fear when “[p]assengers can make a false complaint against you—because they are Islamaphobic, racist—and you will be deactivated. Your allegations don’t even have to be factual. Uber doesn’t even give you the respect to investigate the allegations about you.” Certain drivers contrast the severe penalties they face when passengers allege driver misconduct with the lack of consequences for passengers when drivers allege passenger misconduct. In a mix of anger and despair, Issa an Uber and Lyft driver, asks: “Having Uber say to you, someone who physically assaults you—that you won’t be matched with this person again. Are you serious?”

Working for a black box algorithm leaves many drivers feeling a profound lack of agency. Some drivers describe working on the app like gambling, likening the blips, beeps, and nudges urging drivers to continue driving, to “casino sounds.” Others describe working on the app like “sharecropping.” Still others describe the experience as “like slavery.” Each driver’s interpretation is individual, but what is striking is the frequency with which drivers, in describing their labor, resort to words that express their painful exclusion from the social contract of work.
Data and Evidence

Q4b What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers' pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?

Workers’ Pay, Benefits, and Employment

Uber and app-based corporations like Lyft that adopted a similar business model, are some of the most prominent examples of how automated worker surveillance and management systems can erode drivers’ capacity to earn a decent living.57 A key strategy Uber used to gain early market dominance was to get passengers to expect an “on-demand” ride.58 Uber achieved this by adopting technology so that virtually anyone with a car could work on their app, thus flooding the market with drivers and exerting tremendous downward pressure on drivers’ wages.59

Uber and Lyft have used their algorithms to push drivers’ wages so low that it’s nearly impossible for drivers to make enough to even support one person, let alone a family.60 According to a nationwide study published in 2022, nearly two-thirds of gig workers nationwide earn less than $15 per hour and 29% earn less than the minimum wage in their state.61 Similarly, a 2022 study in Denver found that drivers for Uber, Lyft, and DoorDash take home only $5.49 per hour after expenses, working in a city with a minimum wage of $15.87.62 A 2022 California study found that Uber and Lyft drivers take home an average of only $6.20 per hour after subtracting expenses and the cost of key benefits not afforded to drivers.63

Further exacerbating their financial insecurity, drivers may be deactivated by the app unpredictably and for seemingly arbitrary and opaque reasons.64 A 2023 survey of over 800 California drivers found that two-thirds of those surveyed had been deactivated temporarily or

---

57 Rogers, supra note 6, p. 7.
58 Ibid.
59 Ibid.
60 Ibid.
61 A 2022 Colorado study found that 59% of drivers supported at least one other person. E. Leverage et al., The Gig Gap: The Reality of Denver Gig Workers, Colorado Jobs with Justice (Oct. 4, 2022), p. 5, https://tinyurl.com/yjcjub2c.
63 Leverage, supra note 60, p. 5.
65 U.S. Terms of Use, Uber (Jan. 17, 2023), Termination. §1 (reserving right to “terminate these Terms or any Services with respect to you … at any time for any reason), https://tinyurl.com/2p9zh88h; Lyft Terms of Service, Lyft (Dec. 12, 2022), Termination, § 16 (reserving right to immediately deactivate if “you fall below Lyft’s star rating or cancellation threshold”), https://www.lyft.com/terms.
permanently.\textsuperscript{65} A national survey of over 900 drivers found that 40% of respondents had been deactivated in the last year.\textsuperscript{66} Thirty percent of drivers reported the companies failed to provide any explanation for their deactivation.\textsuperscript{67}

For drivers, the consequences of deactivation can be severe. Nearly one in four deactivated drivers responding to the 2023 California survey reported difficulty paying for schooling, childcare, or other child-related expenses.\textsuperscript{68} In the same survey, more than one-quarter of deactivated drivers (28%) experienced difficulty paying medical insurance, medical bills, and costs.\textsuperscript{69} Eighteen percent of drivers reported losing their car after deactivation; devastatingly, as many as 12% of deactivated drivers reported losing their home.\textsuperscript{70}

\textit{Workers’ Physical and Mental Health}

The health and safety crisis among app-based drivers is no accident. Relying on a business model that pays low wages and that shifts responsibility for occupational safety to drivers, Uber and Lyft have created some of the most dangerous jobs in the nation.\textsuperscript{71}

Researchers have coined the term “algorithmic insecurity” to describe the continuous worry and fear that app-based workers experience about their ability to access work, decent pay, and reasonable working conditions when laboring in an unstable and opaque online environment.\textsuperscript{72} The need to work consistently and accept jobs as they become available aggravates stress, as does the financial pressure to overwork or to work irregular hours, which can lead to anger, depressive symptoms, poor sleep, and exhaustion.\textsuperscript{73} Researchers have also observed that the platforms’ so-called ‘gamification’ techniques of unpredictably eliciting drivers to accept consecutive challenges to unlock financial rewards resemble techniques to promote compulsive gambling.\textsuperscript{74} The constant surveillance and management of workers through the app

\begin{footnotesize}
\begin{itemize}
\item[65]\textit{Fired by an App}, Asian Americans Advancing Justice-Asian American Law Caucus and Rideshare Drivers United (Feb. 2023), p. 4, \url{https://tinyurl.com/mrxutfpn}.
\item[66]\textit{Driving Danger: How Uber and Lyft Create a Safety Crisis for their Drivers}, The Strategic Organizing Center (Apr. 20, 2023), p. 15, \url{https://tinyurl.com/36t7ud9a}.
\item[67]\textit{Fired by an App, supra} note 65, p. 4.
\item[68]Id., p. 18.
\item[69]Ibid.
\item[70]Ibid.
\item[71]P. Leigh, \textit{Open Forum: Driving for Uber, Lyft, GrubHub and others is one of the most dangerous jobs in the country}, San Francisco Chronicle (Jul. 25, 2019), \url{https://tinyurl.com/49ts4w3h}.
\end{itemize}
\end{footnotesize}
substitutes for interpersonal explanation of an automated decision, leaving many drivers feeling ignored and isolated, with negative mental health consequences.\textsuperscript{75}

App-based work is also physically dangerous. According to a 2023 survey of over 900 Uber and Lyft drivers nationwide, two-thirds of all rideshare drivers reported being threatened, harassed, or assaulted in the last year.\textsuperscript{76} A majority of driver respondents reported being verbally abused;\textsuperscript{77} more than a quarter reported being verbally threatened with physical harm, and more than 14% reported being grabbed, groped, or hit.\textsuperscript{78}

Even worse, the combination of Uber’s and Lyft’s algorithmic systems of low pay and frequent and seemingly arbitrary deactivations strongly incentivize drivers to drive passengers who appear too drunk to transport safely, are behaving unpredictably, or are requesting a ride that feels like a set-up for a potential robbery or assault. The same 2023 national survey found that the most common reason for accepting a ride that made drivers feel unsafe—cited by 59% of drivers—was fear that passengers might leave negative reviews leading to deactivation.\textsuperscript{79} Another 49% of drivers reported accepting unsafe rides out of fear that their cancellation rates would rise above acceptable levels; and another 43% reported accepting unsafe rides out of fear their acceptance rates would fall too low.\textsuperscript{80} More than half (57%) of drivers also reported accepting unsafe rides because they feared losing income.\textsuperscript{81}

The stakes of this health and safety crisis could not be higher. A review of press reports, police reports, and court records reveals that in 2022 alone, at least 31 app-based drivers and delivery workers were murdered on the job.\textsuperscript{82} Similar research found that over 50 drivers were killed on the job between 2017-2022.\textsuperscript{83} The true numbers may be higher, as these numbers are based on the public record alone, and in nearly every state, app-based corporations are not required to report instances of violence, assault, workplace injury, or homicides to government agencies.\textsuperscript{84} Even so, if the United States Bureau of Labor Statistics treated app-based work as a sector, it would likely be among the top five sectors where workers are killed on the job.\textsuperscript{85}

\begin{flushright}
Vignola
\end{flushright}

\textsuperscript{76} \textit{Driving Danger}, supra note 66, p. 7.
\textsuperscript{77} \textit{Ibid}.
\textsuperscript{78} \textit{Ibid}.
\textsuperscript{79} \textit{Driving Danger}, supra note 66, p. 12–13.
\textsuperscript{80} \textit{Ibid}.
\textsuperscript{81} \textit{Ibid}.
\textsuperscript{84} \textit{Murdered Behind the Wheel}, supra note 82, p. 9.
\textsuperscript{85} \textit{Ibid}.
Workers’ Ability to Exercise Workplace Rights

Automated workplace management and surveillance tools also impact drivers’ ability to exercise their rights collectively. Even accounting for gig workers’ higher levels of financial strain, researchers report increased powerlessness and loneliness among app-based workers, concluding that algorithmic control and distancing strategies may undermine worker autonomy and meaningful connection— which can play a key role in building collective demands.

When drivers raise their collective concerns, this same social and spatial isolation can also make it more difficult for workers to have their voices heard. As legal scholar Brishen Rogers highlights, app-based workers currently do not have the right to use their employer’s website, app, or other technological platform to communicate with the public. As Rogers explains, “there simply is no digital equivalent to the in-person picket line or leafleting effort on or near the employer’s physical property.” Rogers directly contrasts drivers’ lack of access to such a space with the out-sized power of app-based companies to use that same digital space as a megaphone for their own ends. Uber and Lyft inundated drivers and passengers with in-app messages to support Proposition 22, a 2020 California ballot initiative that reduced drivers’ employment rights. This spring, Uber emailed Minnesota drivers and passengers with links to state lawmakers urging them to oppose a drivers’ rights bill.

As data surveillance technologies become cheaper and more ubiquitous, app-based corporations will be increasingly capable of building large, aggregated, data profiles that allow them to screen for nascent organizing efforts, or for workers more likely to participate in collective action. This reality may not be far off. Uber already receives geofence warrant requests, which can use smartphone data to collect the identities of people at protests and other large-scale political events. Conceivably, companies could use such data to screen out prospective workers they deem unlikely to defer to management authority. As Rogers highlights, under current law, workers and even regulators may struggle to identify or access the underlying surveillance algorithms to even determine if such practices are occurring.

---

87 Rogers, supra note 6, p. 95.
88 Ibid.
91 Rogers, supra note 6, p. 99.
93 Rogers, supra note 6, p. 97.
94 Id., p. 98.
Q4d: What data and evidence exist on how the impact of automated worker surveillance and management systems differs across groups of workers, including based on characteristics such as race, national origin, [or] sex?]

Q4e: What data or evidence exists on whether automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination?

The big data algorithms used by Uber, Lyft, and other app-based corporations both preserve and amplify the deep racial and gender inequalities that pervade the present, while also magnifying the power of corporations over workers.95 This Section addresses five aspects of such automated surveillance and management systems: (1) facial recognition technologies, (2) passenger reviews of drivers, (3) driver health and safety, (4) driver deactivations, and (5) algorithmic wage discrimination. As legal scholar Ifeyoma Ajunwa warns, “Governmental action is necessary to ensure that the future of work is not a dystopia for all workers, but especially for more vulnerable workers of color.”96

**Facial Recognition Technologies**

From the instant app-based drivers log on to the app, Uber and Lyft use automated algorithms and facial recognition technologies to verify drivers’ identities, despite this technology being notoriously inaccurate for non-white and non-male faces.97 If the automated system fails to recognize the driver’s face, the driver can be locked out of the app, and may be deactivated. In recent years, drivers of color in the United States and the United Kingdom have brought legal action against Uber, alleging racial discrimination because the app failed to recognize their faces and prevented them from working.98 A 2021 Los Angeles Times investigation similarly found that some transgender Uber drivers were deactivated after the app deemed their post-transition profile photos to be “fraudulent.”99

---

95 See generally, Milner, *supra* note 8.
Passenger Reviews of Drivers

Despite mounting evidence of racially biased outcomes, Uber, Lyft, and other app-based platforms rely heavily on systems in which passengers are asked to rate drivers after each ride in order to monitor and discipline drivers. Uber and Lyft drivers who receive insufficiently high passenger ratings are at risk for deactivation. Black and brown app-based drivers report receiving lower ratings from passengers than white drivers, opening up what some researchers have described as a backdoor to discrimination.

This problem is long-standing. A 2016 study by Data & Society documents how Uber and other app-based corporations’ reliance on potentially biased passenger ratings may lead to a disparate impact in workplace outcomes. Legal scholar Richard Ford has described how such bias may be particularly pernicious in the context of algorithmic management, because the numeric rating gives the illusion of data-driven objectivity, while stripping the interpersonal evaluation that undergirds the rating of its social context. This both makes it easier for customers to hurt workers and harder for workers to prove discrimination.

Examples of passenger bias against drivers are all too frequent. In a national survey of over 900 app-based drivers, 39% of drivers of color reported being called a racial, ethnic, or religious slur by passengers. In a California survey of more than 800 current and former Uber and Lyft drivers, 50% of drivers reported experiencing bias or discrimination from passengers based on their race or national origin; and of those drivers, 50% reported that the passenger had filed a complaint against them with Uber or Lyft.

Given the weight Uber’s and Lyft’s algorithms give to racially biased customer reviews and complaints, it is shocking but not surprising that drivers of color report being disproportionately deactivated. A study by Asian American Advancing Justice–Asian Law Caucus and Rideshare Drivers United found that drivers of color were significantly more likely than white drivers to have their accounts deactivated after passenger complaints. Of the 810 drivers surveyed, 69% of drivers of color reported experiencing either permanent or temporary

---

100 Lyft Terms of Service, supra note 64 (reserving right to immediately deactivate if “you fall below Lyft’s star rating”); Uber Community Guidelines, Uber (Oct. 20, 2021) (stating that “drivers … that don’t meet the minimum average rating for their city may lose access to all or part of the Uber Marketplace Platform”), https://tinyurl.com/3pz5p9hw.


103 Ibid.

104 Harnett, supra note 101.

105 Ibid.

106 Driving Danger, supra note 66, p. 9.

107 Fired by an App, supra note 65, p. 4.

108 Ibid.
deactivation, in comparison with 57% of white drivers.\textsuperscript{109} Forty-two percent of deactivated drivers were told their deactivations were due to customer complaints.\textsuperscript{110}

\textit{Driver Health & Safety}

The endemic violence directed towards app-based drivers has generated a racialized safety crisis. According to a 2023 national survey, app-based drivers of color experience violence, harassment, and threats from passengers at higher rates than white drivers.\textsuperscript{111} Sixty percent more drivers of color reported being robbed or carjacked in the last year compared to white drivers.\textsuperscript{112} Drivers of color were also 86% more likely than white drivers to report being called a racial, ethnic or religious name or slur.\textsuperscript{113} One in five drivers of color report being physically grabbed, groped or hit, which is 37% more than white drivers.\textsuperscript{114} Drivers of color also report being verbally threatened with physical harm 24% more than white drivers, and are three times more likely than white drivers to have been shot or stabbed in the last year.\textsuperscript{115} Of the 31 app-based drivers researchers identified as murdered on the job in 2022, 77% were people of color.\textsuperscript{116}

App-based drivers also experience high rates of sexual harassment and assault while working on the platform. In a 2023 survey of California drivers, 43% of drivers reported experiencing sexual harassment on the job (53% of female drivers, 41% of male drivers).\textsuperscript{117} In a 2023 national survey, 27% of drivers reported being sexually propositioned, 14% reported being physically grabbed, groped, or hit, and 3% reported being sexually assaulted or raped.\textsuperscript{118}

The alarming rates of violence that app-based drivers of color experience are rooted in Uber’s and Lyft’s algorithmic management systems. Because of the higher rates of bias they face from customers,\textsuperscript{119} drivers of color are acutely aware that if they cancel a ride with a threatening passenger and later receive a negative review or complaint, they may be summarily deactivated.\textsuperscript{120} In the 2023 national survey, a higher percentage of drivers of color—64% as compared to 55% of white drivers—reported providing rides to threatening passengers.\textsuperscript{121} Drivers of color were also 30% more likely than white drivers (74% vs. 54%) to report having provided a ride to a passenger in the last year who made them feel unsafe due to concerns that
the passenger might leave negative reviews.\textsuperscript{122} Drivers’ documented experiences demonstrate how the disparate impacts of Uber’s and Lyft’s automated management systems push drivers of color into situations in which they face a heightened risk of being victimized by passengers.

\textbf{Deactivations}

One of the most salient features of the automated surveillance and management systems of Uber, Lyft, and other app-based corporations, is just how swiftly and frequently drivers can be deactivated—at times, seemingly based on passenger whims—while in contrast, passengers generally face much less intensive discipline.\textsuperscript{123} As journalist, researcher, and activist, Dalia Gebrial explains, Uber’s and Lyft’s deactivation systems draw on long-held, racially biased tropes of guilt and innocence, to configure drivers—who are racialized and gendered as black and brown men—as being a “threat” or “risky,” and passengers—who are racialized as white and more likely female—as being “threatened” or “at risk.”\textsuperscript{124} Thus, while Uber and Lyft drivers must submit photo identification, pass driving and criminal background checks, and satisfy other requirements, passengers can download the app and create an account without any such verifications.\textsuperscript{125} Similarly, while drivers can rate and report passengers for misconduct, this mostly does not result in deactivation.\textsuperscript{126}

Significantly, the asymmetric burden of compliance that app-based companies’ automated systems impose on drivers, does not map onto the actual, relative health and safety risks to drivers and passengers of using these platforms.\textsuperscript{127} Uber’s own internal reports in 2019 and 2020, show that drivers are nearly as subject to assault from passengers as passengers are from drivers.\textsuperscript{128} Further, as sociologist Elizabeth Anne Watkins highlights, despite the fact that many of Uber’s driver surveillance and management technologies were rolled out in the name of passenger safety, Uber has yet to publish any data on whether these interventions have had any impact on account fraud or passenger safety.\textsuperscript{129}

As described in an investigation by the non-profit news organization, \textit{The Intercept}, recent artificial intelligence patents filed by Uber reinforce the company’s pattern of experimenting with algorithmic prediction and driver surveillance systems in the name of passenger safety.\textsuperscript{130} These new systems also raise concerns that they could result in unjust or biased deactivations of drivers, including immigrants and drivers of color. One patent for scoring

\textsuperscript{122} Id., p. 13.
\textsuperscript{123} Gebrial, \textit{supra} note 5, p. 16.
\textsuperscript{124} Id., p. 16–17.
\textsuperscript{125} Watkins, \textit{supra} note 32, p. 52:12.
\textsuperscript{126} Gebrial, \textit{supra} note 5, p. 17.
\textsuperscript{127} Watkins, \textit{supra} note 32, p. 52:17.
\textsuperscript{129} Watkins, \textit{supra} note 32, p. 52:17.
\textsuperscript{130} B. Lin, \textit{Uber Patents Reveal Experiments with Predictive Algorithms to Identify Risky Drivers}, The Intercept (Oct. 30, 2021), \url{https://tinyurl.com/mr36ycue}. 

1290
driver safety risk suggests a passenger’s reporting they could not understand the driver’s “heavy accent” can be an indicator of “low-quality” service. Another patent aims to predict safety incidents using criteria which include, among others, passenger ratings and a driver’s social network peers. But passenger reviews can be biased. And to the extent immigrant drivers and drivers of color are more likely to be socially connected to drivers living in lower-income neighborhoods, those neighborhoods tend to have a higher degree of traffic crashes than affluent neighborhoods, research indicates, not because of driver safety, but because of the greater prevalence of hazards in the built environment and of older vehicles without safety features. Yet another Uber patent develops an individual “driver safety score,” which, if unsatisfactory, can be a basis for “intervention.” According to the patent, driving at night is a factor that could negatively impact a score, in comparison to driving during the day. But if drivers who drive at night are more likely to be drivers of color and immigrants because they tend to hold down multiple jobs or drive longer hours, these groups could theoretically be penalized with lower scores, and be vulnerable to intervention.

As Gebrial highlights, the manufactured construction of app-based drivers as public safety threats is deployed to justify the logic that drivers’ behavior must be minutely quantified and subject to constant scrutiny. This surveillance apparatus provides the pre-conditions for Uber’s, Lyft’s and other app-based companies’ swift and heavy-handed driver deactivations, which in turn, create a more disposable, exploitable, heavily disciplined, workforce of vulnerable black and brown drivers. Ironically, the rhetoric of safety becomes a way to make app-based drivers’ already risky jobs even more dangerous by subjecting them to ever more precarious working conditions.

**Algorithmic Wage Discrimination**

Automated worker surveillance and management systems can produce outcomes that result in unlawful discrimination when they function as “black boxes” with internal workings not clear to most people, including, in some cases, even the developer of the tool. The “black boxes” at the center of other app-based corporations’ automated systems are the algorithms they

---

135 Ibid.
136 Ibid.
138 Id., p. 17.
139 Id., p. 2.
use to allocate rides to drivers and to determine driver compensation. These automated pay algorithms allocate individualized, temporary financial bonuses to drivers, which many drivers view as essential to supplement their otherwise inadequate earnings. These algorithms, which personalize wages based on driver data, are proprietary, and thus, unknowable to drivers. In a phenomenon legal scholar Dubal has described as “algorithmic wage discrimination,” the apps create a system in which drivers doing the same work, with the same skill, for the same company, at the same time, may earn very different hourly pay.

As Dubal explains, the large amounts of data on driver behavior at app-based corporations’ disposal, along with their growing technological sophistication, create the ever-increasing possibility that their algorithms can “calculate the exact wage rates necessary to incentivize desired behaviors.” Thus, “algorithmic wage discrimination allows firms to personalize and differentiate wages for workers in ways unknown to them, paying them to behave in ways that the firm desires, perhaps [paying] as little as the system determines that they may be willing to accept.” Dubal describes examples of drivers being forced to wait for 45 minutes in a busy area to get dispatched the final ride to qualify for a $100 bonus, or being subjected to a kind of “casino mechanics” in which the hope of being dispatched a lucrative ride keeps drivers on the road for longer.

Dubal points out that “even if on-demand companies are not using algorithmic wage discrimination to offer vulnerable workers lower wages based on their willingness to accept work at lower prices, the possibility remains that they can do so.” Even more alarmingly, due to the opacity and increasing complexity of their systems, there is no real way for workers, the public, or in some instances, even regulators, to verify that they are not doing so. A recent Uber patent illustrates the company’s growing electronic surveillance and AI capacity, describing a “service data store,” which may “store data about services provided by multiple providers [or drivers],” which “may include an origin (e.g., start location), destination, estimated duration, actual duration, route …, date, time, value [i.e., the amount of compensation a driver receives for a service], incentives offered to a provider [driver], geographical regions through which a route passed, traffic conditions, etc.” According to the patent, “[s]ervice data may be used … to predict values [or compensation a driver receives for a service] for individual services based on past service or values” and “[h]istorical and recent service data is used to improve predicted value [compensation] estimations for individual services and to improve estimates related to likelihood that providers will travel across geographical regions.”

---

141 Vignola, supra note 21, p. 4.
143 Id., p. 6.
144 Ibid.
145 Id., p. 36.
146 Id., p. 40.
147 Ibid.
149 Ibid.
Some qualitative research already documents app-based drivers’ anecdotal experiences that as they drive more on the platforms—and thereby signal greater economic desperation—they receive fewer financial incentives.\textsuperscript{150} As more data on drivers’ activities both inside and outside of work is collected and sold among corporations, a scenario becomes increasingly plausible in which app-based corporations could feed outside data, such as credit card debt or court judgments into their algorithms to pin-point which workers are the most financially desperate, and thus the most likely to accept the lowest compensation.\textsuperscript{151} App-based companies already partner with financial services institutions to offer drivers bank accounts, credit, and debit cards.\textsuperscript{152}

By engaging in algorithmic wage discrimination, Uber’s and Lyft’s platforms upend deeply rooted principles of equal pay for equal work and of the fairness and predictability of wages.\textsuperscript{153} In one driver’s words: “[E]very single day they are figuring out how to exploit you in different ways . . . The state of work is going to deteriorate in this country in such a way that it’s not recognizable anymore. It already is.”\textsuperscript{154}

\textbf{Q4k: Where might further research, including by the Federal government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?}


“Sami’s Law” requires the GAO to submit to Congress a biennial report with the results of a study on fatal and non-fatal physical and sexual assaults against drivers and passengers using app-based and other for-hire vehicles. (34 USC § 41313(a)(1).) The study must also include the safety steps taken by app-based corporations and other for-hire vehicles services related to rider and driver safety. (34 USC § 41313(a)(3).) The GAO study should include an analysis of current automated surveillance and management practices that may increase the risks of assault on these platforms, and safety steps that can mitigate these risks.

\begin{itemize}
\item \textsuperscript{150} A. Zhang et al., \textit{Algorithmic Management Reimagined for Workers and By Workers}, CHI Conference on Human Factors in Computing Systems, New Orleans, LA (Apr. 2022), \url{https://tinyurl.com/msf4f5c7} (noting “Drivers unanimously agreed that Quest [bonus] offers were determined by the frequency of driving, drawing from personal and other driver experiences: the more a driver worked, the worse the bonus offers they would receive”).
\item \textsuperscript{151} M. Cerullo, \textit{How companies get inside gig workers’ heads with ‘algorithmic wage discrimination}, CBS News (Apr. 18, 2023), \url{https://tinyurl.com/2p8e4myy}.
\item \textsuperscript{153} \textit{Id.}, p. 12.
\item \textsuperscript{154} \textit{Id.}, p. 39.
\end{itemize}
**Fund New Research into the Effect of Automated Surveillance and Management Technologies on App-Based Workers’ Health and Safety**

Existing research and workers’ experiences indicate that automated surveillance and management systems have a variety of negative impacts on app-based workers. However, additional research could be useful to understand the effects of automated surveillance and management systems on: (1) app-based workers’ mental and physical health, (2) app-based workers’ experiences with deactivation, (3) app-based workers’ earnings and financial insecurity, including algorithmic wage discrimination, and (4) any differential impacts based on characteristics such as race, national origin, sex, age, disability, religion, or health status.

**Fund Community-Based Participatory Research**

Although there is a growing body of research on app-based drivers produced by academics and think-tanks, comparatively little research has been produced with app-based drivers, centering their perspectives in the definition of problems and potential solutions. Funding for community-based participatory research (CBPR) projects with driver-led organizations could help close this gap. CBPR emphasizes researchers’ equitable engagement with community partners throughout the research process, from problem definition, through data collection and analysis, to the use of findings to help effect change. CBPR initiatives have been highly effective in bridging “street science” with academic-based evidence and advocacy. They have been supported by the federal government in contexts ranging from public health, to housing, and the environment. Findings from CBPR initiatives could be compiled into regional, statewide, or nationwide datasets and analyses.

**Harness and Expand Existing Statistical Surveys**

The Department of Labor, through the Office of the Assistant Secretary for Policy and the Bureau of Labor Statistics, and the Commerce Department, through the Census Bureau and the Bureau of Economic Analysis, should be instructed to improve data collection through business and household surveys and other research tools on the app-based economy. Worker-led organizations, and researchers and academics aligned with app-based workers should be consulted both initially and on an ongoing basis on how to make such improvements, to ensure they reflect ongoing shifts in the app-based worker environment.

---


157 Ibid.

Policies, Practices, or Standards

Q5c: What policies or actions should Federal agencies consider to protect workers' rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

While app-based companies’ automated worker surveillance and management systems may be relatively new, the social harms workers experience as a result of these practices—low and unfair pay, lack of benefits, biased and arbitrary discipline and firings, health and safety threats, and insecurity are not. Federal agencies, through regulations, enforcement, contracting, and grantmaking, can act now to address these social harms.

Policy, Regulation and Enforcement

Given the extreme lack of transparency in app-based corporations’ algorithmic decision-making and surveillance systems to both workers and the general public, the federal government and other regulators are uniquely positioned to investigate abuses wrought by these corporations and enforce violations when they are found.

- **Issue Final Rulemaking on Classifying Employees, Independent Contractors:** The Department of Labor (DOL) should move forward expeditiously with final rulemaking on its October 13, 2022, Notice of Proposed Rulemaking (NPRM) on the classification of employees and independent contractors, including identifying automated worker surveillance in its discussion of control reserved or exerted through supervision.\(^{159}\)

- **Prevent and Address Antitrust Violations:** The Federal Trade Commission (FTC) should continue to prioritize preventing and remedying antitrust violations in the app-based economy, consistent with its September 15, 2022, *Policy Statement on Enforcement Related to Gig Work*.\(^{160}\) This includes, but is not limited to, investigating and enforcing unfair or deceptive practices involving automated or algorithmic decision-making.\(^{161}\)

- **Prevent and Address Consumer Violations:** The Consumer Financial Protection Bureau (CFPB) should continue to prioritize preventing, investigating, and remedying consumer violations in the app-based economy, including, but not limited to certain actions by

---


\(^{161}\) Id., p. 10.
surveillance companies involving the tracking and sale of worker data may be violating the Fair Credit Reporting Act and other consumer financial protection laws.162

- **Address Exemption for Worker Organizing Activities from Antitrust**: Consistent with the September 28, 2021 letter to Congress from FTC Commissioner Lina Khan and Commissioner Bedoya’s April 28, 2023, address, the FTC should work with the Department of Justice’s Antitrust Division to provide guidance to courts regarding the exemption of “worker organizing activities from antitrust.”163

- **Convene an Interagency Task Force on App-Based Workers**: A Task Force should be created to identify federal agency policies, practices, and programs that could be used to promote app-based worker voice and job quality as well as to address harms app-based workers—and particularly, workers of color—experience from automated management and surveillance systems. A number of federal government agencies have taken some initial steps to prioritize these challenges, but these challenges are a matter of national interest, requiring a coordinated response.

- **Launch a Gig Worker Outreach Initiative**: Consistent with their recent announcements to expand enforcement of app-based workers’ legal protections nationally,164 the DOL, the National Labor Relations Board (NLRB), the FTC, and the CFPB should: (1) expand national and regional outreach to app-based workers, and (2) post updated, visible, and accessible materials on agency websites, worker.gov, and social media platforms on app-based workers’ rights and on how to report potential workplace issues to the government.

**Contracting and Grantmaking**

- **Assist App-Based Platform Cooperatives**: Relevant agencies should invest in revolving loan funds or grant programs that make low- or no-cost financing available to worker-owned, app-based cooperatives165 and to the technical assistance organizations that support them.

- **Assist Workers Centers and App-Based Worker-Led Organizations**: Relevant agencies should invest in grant programs to support workers centers and app-based worker-led organizations. These organizations relieve stressors on app-based workers by supporting

---

165 A worker-owned, app-based cooperative is a website or mobile app designed to provide a service or sell a product that is collectively owned and governed by the people who depend on and participate in it. Platform Cooperatives, Univ. of Wisconsin Center for Cooperatives, https://tinyurl.com/5t2sutan (last visited Jun. 23, 2023).
connections to the social safety net, improving financial literacy, lessening social isolation, and educating and providing app-based workers with information on their rights.

- **Explore Opportunities for Enhancing App-Based Workers’ Job Quality Through Federal Contracting:** Relevant agencies should identify contracting opportunities where they can incorporate job quality elements, disclosure or information requirements regarding the use of automated management or surveillance systems, and other mechanisms to enhance job opportunities for app-based workers. Relevant agencies should also evaluate establishing procurement policies to provide preferential treatment of platform app-based cooperatives over privately owned app-based platforms.\(^{166}\)

    As the federal government continues its work of assessing automated surveillance and management systems, we welcome any future opportunities for collaboration. This includes offering analyses, resources, or guidance in developing policies, programs, and best practices. Thank you for your review and consideration of this response.

Sincerely,

PowerSwitch Action\(^{167}\)
Chiago Gig Alliance/The People’s Lobby\(^{168}\)
Colorado Independent Drivers United-CWA\(^{169}\)
Gig Workers Rising\(^{170}\)

---

\(^{166}\) In late 2020, the General Services Administration awarded Uber and Lyft a five-year federal contract worth up to $810 million. T. Bellon, *U.S. federal government awards transportation contract to Uber, Lyft*, Reuters (Nov. 23, 2020), [https://tinyurl.com/3fpctwdk](https://tinyurl.com/3fpctwdk).

\(^{167}\) PowerSwitch Action ([www.powerswitchaction.org](http://www.powerswitchaction.org)) is a national network of leaders, organizers, and strategists organizing to realize and build multiracial feminist democracies in our cities, towns, and regions.

\(^{168}\) The Chicago Gig Alliance/The People’s Lobby ([www.thepeopleslobbyusa.org](http://www.thepeopleslobbyusa.org)) is a membership-driven organization of people across the Chicago region that work together to build widespread support for public policies and candidates that put racial and gender justice and the needs of people and the planet first.

\(^{169}\) Colorado Independent Drivers United-CWA ([https://cidu-cwa7777.org](https://cidu-cwa7777.org)) is a union of Rideshare, Delivery, Taxi, and Limousine drivers organizing for just wages and better working conditions.

\(^{170}\) Gig Workers Rising ([https://gigworkersrising.org](https://gigworkersrising.org)) is building a movement to support app-based workers who are organizing for better wages, working conditions, and respect on the job.
Artists and writers are having their work involuntarily used as members of datasets in the creation of models that will ultimately remove jobs and reduce their rights as workers, ultimately reducing careers to gig jobs. I am sure you have already heard this, but Netflix is acting as a holdout in the WGA strike.
Hi,

As a brief introduction, I'm a professor at GW and saw the recent call for information about automated tools in the workplace. I did my Ph.D. in business ethics at The Wharton School at University of Pennsylvania. My research is on technology ethics and policy. In the last few months, I spoke at the recent Wall Street Journal Risk and Compliance Forum about chatgpt in the workplace (video [here](https://www.youtube.com/watch?v=video_id)), and have been interviewed on topics related to AI and automation in the workplace for Marketplace (public radio interview [here](https://www.marketplace.org/story/ai-bias-audit-law) about New York's new AI bias audit law), Financial Times, etc.

I thought I'd pass on some of my recent research (also attached): *Hiring, Algorithms, Choice: Why Interviews Still Matter*.

Most of the research thus far on algorithms and AI in the workplace have focused on bad outcomes—inaccurate judgments, sexist or racist outcomes, etc. In this work, I focus on the ethical concerns that remain, even if, ultimately there are technical solutions that improve these bad outcomes.

This is the gist of that above article: “Even if concerns around data and bias in AI software are ultimately improved through an engineering solution, it still doesn’t settle the question of whether HR managers should defer to algorithms. This is not because our gut instincts are far superior—often they’re not,” Bhargava says. “Rather, this is because there are important (and overlooked) ethical values created through us making choices—including choices about whom to work with or not work with—that would be jeopardized, were HR managers to abdicate that choice to an algorithm. This is so, no matter how sophisticated algorithms ultimately become at predicting the fit and performance of an employee.”

Please don't hesitate to reach out if I can be of any assistance as you navigate these deeply important issues.

Warmly,

Vik

--

Vikram R. Bhargava, Ph.D.
Assistant Professor of Strategic Management & Public Policy
George Washington University School of Business
Hiring, Algorithms, and Choice: Why Interviews Still Matter

Vikram R. Bhargava
George Washington University, USA

Pooria Assadi
California State University, Sacramento, USA

Why do organizations conduct job interviews? The traditional view of interviewing holds that interviews are conducted, despite their steep costs, to predict a candidate’s future performance and fit. This view faces a twofold threat: the behavioral and algorithmic threats. Specifically, an overwhelming body of behavioral research suggests that we are bad at predicting performance and fit; furthermore, algorithms are already better than us at making these predictions in various domains. If the traditional view captures the whole story, then interviews seem to be a costly, archaic human resources procedure sustained by managerial overconfidence. However, building on T. M. Scanlon’s work, we offer the value of choice theory of interviewing and argue that interviews can be vindicated once we recognize that they generate commonly overlooked kinds of noninstrumental value. On our view, interviews should thus not be entirely replaced by algorithms, however sophisticated algorithms ultimately become at predicting performance and fit.

Key Words: ethics of interviews, hiring ethics, employment ethics, recruiting automation, algorithmic ethics, algorithmic decision systems

Why do organizations conduct job interviews, despite the enormous costs associated with the interview process? At first blush, this does not seem like an especially challenging question. This is because a natural and seemingly obvious answer immediately comes to mind: interviews are for predicting a candidate’s future performance and fit with respect to the hiring organization’s requirements, values, and culture—that’s why organizations conduct interviews, despite their costs (Cappelli, 2019b; Elfenbein & Sterling, 2018; Muehlemann & Strupler Leiser, 2018; Society for Human Resource Management [SHRM], 2017). This is also the traditional view of interviewing espoused by managers and is how the nature and function of interviews are characterized in human resource management (HRM) textbooks (Dessler, 2020; Mathis, Jackson, Valentine, & Meglich, 2016; Mondy & Martocchio, 2016).1 Thus,

---

1 This is not to say that all contemporary HRM scholars necessarily endorse the efficacy of interviews toward their stated ends. Indeed, a number of HRM scholars doubt the effectiveness of interviews toward
although the costs may be undesirable, they are the price to pay, as it were, to be able to judge whether a candidate will match the needs of the role and the organization. In this article, we suggest that the question of why to conduct interviews is a more difficult one than it first seems. The force of this question can be appreciated when juxtaposed against a twofold threat we argue the traditional view of interviewing faces. The first threat, the behavioral threat, holds that a large body of behavioral evidence suggests that we are poor predictors of future performance and bad judges of fit. This is for multiple reasons: the judgments of interviewers are riddled with biases, interviewers overestimate their assessment capacities, and organizations rarely assess the performance of candidates they might have passed on (in relation to the candidates they ultimately selected). As one HRM textbook notes, “traditionally, interviews have not been valid predictors of success on the job” (Mondy & Martocchio, 2016: 165). In short, those involved in making hiring decisions are demonstrably bad at predicting future performance and assessing fit.

The behavioral threat has brought some management theorists to suggest abandoning interviews as traditionally conceived (i.e., unstructured interviews) and moving toward structured interviews. Yet structured interviews, too, face problems: they can collapse into unstructured interviews, or alternatively, they start out unstructured either before or after the official start of the interview and, in doing so, increase exposure to the behavioral threat. More fundamentally, the behavioral threat is simply pushed back one step, to the point at which one decides the structure of the interview. Thus, although structured interviews may be an improvement upon unstructured interviews, they, too, do not fare especially well with respect to the behavioral threat.

A defender of the traditional view might acknowledge the force of the behavioral threat yet still respond, “We have no better alternative!” But this argumentative maneuver is cut off by the second threat the traditional view faces: the algorithmic threat. Algorithms already have a superior track record to humans, even expert humans, of predicting the performance and fit of candidates in a number of domains. Indeed, 67 percent of eighty-eight hundred recruiters and hiring managers globally surveyed by LinkedIn in 2018 noted that they use artificial intelligence (AI) tools to save time in sourcing and screening candidates (Ignatova & Reilly, 2018). So, where does this leave the practice of interviewing?

The behavioral and algorithmic threats, taken together, pose what we call the “interview puzzle” for the traditional view of interviewing. If the traditional view is correct about the nature and function of interviews—that interviews are for predicting the future performance and fit of a candidate with respect to the role’s and organization’s needs—then it seems as though the justification for the practice is predicting future performance and fit. The key point is that, even though a number of HRM scholars are skeptical of the efficacy of interviews at predicting future performance and fit, they nevertheless agree that the nature and function of interviews are for predicting future performance and for assessing candidate fit.

We note that with respect to a range of candidates, especially ones with more experience, the evaluation process is often mutual (i.e., a candidate may be evaluating whether a position at a given firm would satisfy the candidate’s needs).
undermined. Not only is interviewing costly (Cappelli, 2020; Muehlemann & Strupler Leiser, 2018; SHRM, 2017) but we also are bad at it, and we may have better alternatives for predicting performance and fit (i.e., algorithms). Continuing to interview, then, if it is only about predicting performance and fit, seems to be at best an anachronistic human resources (HR) practice or at worst blatant wastefulness sustained by irrational managerial overconfidence. For these reasons, we argue that the traditional view of interviewing must be reexamined.

If interviews were singularly a means to predicting performance and fit, as the traditional view posits, we maintain that the justification for interviews is undermined. However, we argue that the antecedent in this conditional is false: interviews are not singularly a means to predicting performance and fit; rather, they are a much richer normative practice. In particular, we argue that interviews offer different kinds of value that have thus far been overlooked and thus the practice can be worth preserving, despite the behavioral and algorithmic threats. Something of normative significance would be lost were we to abandon the practice of interviewing, and this must be accounted for in our understanding of the nature of interviews.

In other words, we dissolve the interview puzzle by arguing that although the behavioral and algorithmic threats are indeed concerning, they only threaten to undermine our interview practices if the traditional view of interviewing is the whole story. But we argue that the traditional view of interviewing accounts for only part of its function—the parts it overlooks are the other kinds of value that interviews create, and these other kinds of value do not succumb to the behavioral and algorithmic threats. By reframing how we understand the nature of interviews, we advance a broader, normative conception of interviewing that suggests that our ability to choose whom we relate to in the workplace is an important source of value and that our work lives may be worse off without the practice.

We proceed as follows. In section 1, we characterize the traditional view of interviewing and discuss the costs of interviewing that are exhaustively documented in the HRM literature. In section 2, we discuss the behavioral and algorithmic threats and argue that they together undermine the traditional view of interviewing and thus generate the interview puzzle. In section 3, we introduce our value of choice theory of interviewing, grounded in the work of the philosopher T. M. Scanlon (1988, 1998, 2013, 2019). We show how the interview puzzle can be dissolved once we grasp the inadequacy of the traditional view of interviewing: it fails to account for a broader range of contenders for the kinds of value that can be realized through interviewing. If the view we advance is correct, then the current understanding in HRM and management scholarship about the nature and function of interviews must be significantly expanded. In section 4, we offer several clarifications of our account and discuss some potential objections. In section 5, we discuss some new avenues of research that follow from our work. Finally, in section 6, we conclude.

1. THE TRADITIONAL VIEW OF INTERVIEWING

The traditional view of interviewing holds that interviews are one class of selection tools (among other tools, such as tests and background checks) that are useful for
predicting a candidate’s performance and fit. In particular, a selection interview is defined as “a selection procedure designed to predict future job performance based on applicants’ oral responses to oral inquiries” (Dessler, 2020: 207) and is considered a tool for assessing a candidate’s knowledge, skills, abilities, and competencies in relation to what is required for the job (Dessler, 2020; Graves & Karren, 1996; McDaniel, Whetzel, Schmidt, & Maurer, 1994).

Interviews are widespread, in part, because of the belief that they are effective in simultaneously assessing candidates’ ability, motivation, personality, aptitude, person–job fit, and person–organization fit (Highhouse, 2008). Several common assumptions sustain this belief: that making accurate predictions about candidates’ future job performance is possible (Highhouse, 2008); that experience and intuition are necessary in effective hiring (Gigerenzer, 2007); that human beings (i.e., candidates) can be effectively evaluated only by equally sensitive complex beings (e.g., hiring managers), rather than by tests or algorithms (Highhouse, 2008); and that oral discussions with candidates can be revealing, as they allow for “reading between the lines” (Highhouse, 2008: 337).

Despite the widespread use of interviews, they are recognized to be a costly and time-consuming practice. The United States “fills a staggering 66 million jobs a year. Most of the $20 billion that companies spend on human resources vendors goes to hiring” (Cappelli, 2019b: 50). On average, employers in the United States spend approximately $4,000 per hire to fill non-executive-level positions and about $15,000 per hire to fill executive-level positions (SHRM, 2016, 2017), and a substantial portion of these costs is attributed to interviews. Outside the United States, employers report similar experiences. For example, in Switzerland, on average, employers spend as much as 16 weeks of wage payments to fill a skilled worker vacancy, of which 21 percent involves search costs, and roughly 50 percent of the search costs are direct interview costs (Muehlemann & Strupler Leiser, 2018). In addition, significant opportunity costs are associated with interviews for all parties involved (Muehlemann & Strupler Leiser, 2018).

With respect to the time spent on interviews, according to a recent talent acquisition benchmarking report, on average per job, US employers spend approximately eight days conducting interviews (SHRM, 2017). Employers report similar experiences outside the United States. For example, in Switzerland, on average, employers spend approximately 8.5 hours on job interviews per candidate (Muehlemann & Strupler Leiser, 2018).

Of course, the costs of hiring and interviewing are not uniform. The costs vary depending on the skill requirements of the job (Muehlemann & Strupler Leiser, 2018) and the degree of labor market tightness (Davis, Faberman, & Haltiwanger, 2012; Pissarides, 2009; Rogerson & Shimer, 2011), among other factors. That said,

---

3 Two types of fit characterized in a number of HRM textbooks include “person job fit,” the candidate’s fit in relation to the role (Dessler, 2020; Mathis, Jackson, Valentine, & Meglich, 2016; Mondy & Martocchio, 2016), and “person organization fit,” the candidate’s fit in relation to the organization (Dessler, 2020; Mondy & Martocchio, 2016).
these costs on average remain substantial and are increasing—employers today spend twice as much time on interviews as they did in 2009 (Cappelli, 2019b). As costly and time consuming as interviews are, there are also difficulties associated with verifying whether they are worth these costs. Indeed, “only about a third of US companies report that they monitor whether their hiring practices lead to good employees; few of them do so carefully, and only a minority even track cost per hire and time to hire” (Cappelli, 2019b: 50). Even if it were not so difficult to assess whether interviews are worth the costs with respect to the end posited by the traditional view (i.e., predicting performance and fit), two additional threats remain.

2. THE INTERVIEW PUZZLE: THE BEHAVIORAL AND ALGORITHMIC THREATS

2.1 The Behavioral Threat

The traditional conception of interviews—as a means to predict a candidate’s performance and fit in relation to a vacancy—hinges on an important assumption, namely, that performance and fit can be effectively predicted through interviewing. However, a considerable body of knowledge from the social sciences challenges this basic assumption and chronicles the poor track record of predicting performance and fit through interviews (Bishop & Trout, 2005; Bohnet, 2016; Chamorro-Premuzic & Akhtar, 2019; McCarthy, Van Iddekinge, & Campion, 2010; Rivera, 2012). Specifically, although there is empirical evidence that highlights the outsized role interviews have in the hiring process (Billsberry, 2007), interview-based hiring decisions have been found only to account for up to 10 percent of the variation in job performance (Conway, Jako, & Goodman, 1995). Additionally, biases pervade the process of predicting performance and fit through interviews, both in their unstructured and structured formats (Huffcutt, Roth, & McDaniels, 1996; McDaniels et al., 1994).

2.1.1 Unstructured Interviews

Unstructured interviews do not have a fixed format or a fixed set of questions, nor do they involve a fixed process for assessing the given responses (Schmidt & Hunter, 1998). During unstructured interviews, both the interviewer and the candidate investigate what seems most relevant at the time (Bohnet, 2016). This process often produces an overall rating for each applicant “based on summary impressions and judgments” (Schmidt & Hunter, 1998: 267). Unstructured interviews are often...
assumed to be effective in concurrently assessing a range of dimensions associated with predicting performance and person–organization fit (Highhouse, 2008).

However, recent research shows that unstructured interviews may not in fact aid in hiring decisions. This research maintains that unstructured interviews are riddled with biases and are often swayed by the whims of the interviewers (Chamorro-Premuzic & Akhtar, 2019). Specifically, this research suggests that unstructured interviews are ineffective because interviewers tend to overlook the limits of their knowledge (Kausel, Culbertson, & Madrid, 2016), “decide on the fly” what questions to ask of which candidates and how to interpret responses (Cappelli, 2019b: 50), place disproportionate emphasis on a few pieces of information (Dawes, 2001), and confirm their own existing preferences (Chamorro-Premuzic & Akhtar, 2019). Subsequently, they become increasingly confident in the accuracy of their decisions, even when irrelevant information is introduced (Bohnet, 2016; Dawes, 2001). One reason for interviewers’ overconfidence regarding their predictive abilities is that they cannot often ascertain whether, absent interviews, their predictions would turn out to be better or worse, and they would generally lack a large enough sample to deduce any statistically valid inferences (Bishop & Trout, 2005).

While managers more heavily value a given trait or ability if evaluated by unstructured interviews rather than by alternative methods (e.g., paper-and-pencil tests) (Lievens, Highhouse, & DeCorte, 2005), a long-standing body of empirical evidence shows that unstructured interviews are unhelpful with selection decisions. For example, in the context of medical school applications, DeVaul, Jervey, Chappell, Caver, Short, and O’Keefe (1987) compare the students who were initially accepted versus those who were rejected for medical school and find that only 28 percent of the difference between these groups is related to academic and demographic factors and that 72 percent is related to the admissions committee’s preferences developed through interviews. They report that when it comes to attrition and clinical performance during medical school and a subsequent year of postgraduate training, there are no significant differences between the accepted and the rejected groups, suggesting that interviews in this context are unhelpful to the decision-making process. In a similar fashion, Milstein, Wilkinson, Burrow, and Kessen (1981: 77) compare the performance of “a group of 24 applicants who were interviewed and accepted at the Yale University School of Medicine but went to other medical schools … with a group of 27 applicants who attended the same schools but had been rejected at Yale following an interview and committee deliberation.” In this context, too, the researchers find no statistically significant relationship between admission decisions and performance, again pointing to the inefficacy of interviews in aiding the achievement of the decision-making ends.

---

5 Recent research suggests that part of why overconfidence persists, despite its considerable costs, is the status benefits it confers; moreover, these status benefits largely persist, even when the person’s overconfidence is exposed (Anderson, Brion, Moore, & Kennedy, 2012; Kennedy, Anderson, & Moore, 2013).

6 See also Oskamp’s (1965) study of the clinical decisions of psychologists, which shows that the accuracy of their decisions does not increase significantly with additional information from interviews (but confidence in their decision making steadily increases).
Medical school admissions decisions are, of course, not hiring decisions, but similar results are seen in hiring contexts. In a study of the hiring practices at elite professional services firms, Rivera (2012) finds that employers often seek candidates who enjoy similar leisure pursuits and have shared experiences and self-presentation styles. In doing so, Rivera shows that unstructured interviews may be less about assessing knowledge, skills, and abilities and more about exercising biases through replicating ourselves, including, but not limited to, our culture, gender, and ethnicity, in hiring decisions. Finally, through a meta-analysis, Schmidt and Hunter (1998) conclude that unstructured interviews are ineffective at predicting the performance of future employees.

Not only do we know that unstructured interviews are unhelpful in hiring decisions but there is also some empirical evidence that unstructured interviews reliably undermine those decisions (Bishop & Trout, 2005; DeVaul et al., 1987; Eysenck, 1954; Kausel et al., 2016; Milstein et al., 1981; Oskamp, 1965; Wiesner & Cronshaw, 1988). For example, as far back as the middle of the past century, in a large-scale empirical study, Bloom and Brundage (1947) found that the predictive gain in adding an interviewer’s assessment of a candidate’s experience, interest, and personality may well be negative. They specifically report that predictions based on test scores and interviewing were 30 percent worse than predictions based on test scores alone. More recently, Behroozi, Shirolkar, Barik, and Parmir (2020) have shown that even when tests are conducted in interview formats, such as “whiteboard technical interviews” common in software engineering, the mechanics and pressure of the interview context reduce the efficacy of the technical tests. This effect is heightened especially among minorities and other underrepresented groups (Munk, 2021). Other recent research reports similar findings: for example, research on human judgment documents that when decision makers (e.g., hiring managers, admissions officers, parole boards) judge candidates based on a dossier and an unstructured interview, their decisions tend to be worse than decisions based on the dossier alone (Bishop & Trout, 2005). In a similar fashion, Dana, Dawes, and Peterson (2013) show that adding an unstructured interview to diagnostic information when making screening decisions yields less accurate outcomes than not using an unstructured interview at all. In this case, even though the decision makers may sense that they are extracting useful information from unstructured interviews, in reality, that information is not useful (Dana et al., 2013).

2.1.2 Structured Interviews

Unlike the unstructured version, a structured interview involves a formal process that more systematically considers “rapport building, question sophistication, question consistency, probing, note taking, use of a panel of interviewers, and standardized evaluation” (Roulin, Bourdage, & Wingate, 2019: 37) in hiring decisions. In this interview format, to predict good hires, an expert interviewer systematically and consistently poses the same set of validated questions about past performance to all candidates and immediately scores each answer based on a set of predetermined criteria relevant to the tasks of the job (Cappelli, 2019b).
Although structured interviews are available and designed to standardize the hiring process and minimize subjectivity and bias (Bohnet, 2016; Reskin & McBrier, 2000), they are in effect not much more successful than unstructured interviews in aiding hiring decisions for at least three reasons. First, even though structured interviews, in theory, may be less biased and a better predictor of future job performance than their unstructured counterparts, they are not widely adopted in practice (König, Klehe, Berchtold, & Kleinmann, 2010; Roulin et al., 2019). The resistance to structuring interviews (Lievens et al., 2005; van der Zee, Bakker, & Bakker, 2002) is driven by interviewers’ belief that a candidate’s character is “far too complex to be assessed by scores, ratings, and formulas” (Highhouse, 2008: 339) that are predetermined in a structured format.

Second, even in cases when structured interviews are accepted, they are not well implemented for various reasons. For example, structured interviews tend to be more costly to construct (Schmidt & Hunter, 1998) in part because of the difficulties in designing and validating standardized questions and evaluation criteria (Bohnet, 2016; Roulin et al., 2019). Also, in reality, we rarely see structured interviews conducted by trained and experienced interviewers who manage to avoid having their idiosyncratic personalities distort the process (Roulin et al., 2019). Even when structured interviews are conducted by trained and experienced interviewers, the process sometimes deviates to a semistructured or unstructured format. For instance, in conforming to a predetermined set of questions, the flow of conversation in a structured interview might feel stilted, awkward, or uncomfortable for both the interviewer and the candidate, thereby inadvertently shifting the interview process to a less structured format (Bohnet, 2016).

Third, even when structured interviews are conducted by trained and experienced interviewers and the process does not deviate to an unstructured format, empirical evidence shows that structured interviews may not be systematic and free of bias because interviewers may used them to confirm their preexisting judgments rather than to evaluate the candidates—that is, a potential self-fulfilling prophecy (Dougherty, Turban, & Callender, 1994). On the candidates’ side, there is also much room for introducing bias. For example, Stevens and Kristof (1995) show that applicants engage in significant impression management, even in structured interviews, thereby undermining the decision-making process. Furthermore, even when structured interviews are implemented properly, these issues and biases may not be eliminated: they may simply be shifted to the previous step of designing the interview and deciding its structure. Therefore not only are structured interviews rare but, even when they are used and properly implemented, they are afflicted with issues that complicate the evaluation of performance and fit. It is not surprising, then, that Cappelli (2019b: 56) argues that a structured interview is the “most difficult technique to get right.”

7 The average validity of the structured interviews (at about 0.51) is greater than the average validity of the unstructured interviews (at about 0.38) and far greater than the average validity of poorly conducted unstructured interviews (Schmidt & Hunter, 1998: 267).

8 With respect to the predictive power of structured interviews, they “predict performance in job training programs with a validity of about .35” (Schmidt & Hunter, 1998: 267).
Although research shows that interviews can undermine the aims of the hiring process, interviews have remained a popular norm for employee selection for more than a hundred years (Buckley, Norris, & Wiese, 2000; van der Zee et al., 2002). They have remained popular not necessarily because the inefficacy of interviews is unknown. In fact, Rynes, Colbert, and Brown (2002) report that HR professionals appreciate the limitations of interviews. Still, hiring managers remain reluctant to outsource their judgment (Bohnet, 2016).

2.2 The Algorithmic Threat

Interviews, both in their unstructured and structured formats, if not by design, in practice are ineffective at assessing fit or predicting future performance and create a significant opportunity for bias in hiring decisions (Chamorro-Premuzic & Akhtar, 2019; Rivera, 2012). However, proponents of the traditional view of interviewing might respond that there are no alternatives. But this assertion falls short in the face of the second threat the traditional view faces, that is, the algorithmic threat. That is, algorithms, even simple ones, in a number of domains, already are no worse (and are at times superior) at predicting the performance and fit of candidates than humans, even expert humans (Bishop & Trout, 2005; Cappelli, 2020).

Algorithms can be an effective method for predicting future performance and fit primarily because the hiring challenge at its core is a prediction problem, and statistical algorithms are designed to take on and address prediction problems (Danieli, Hillis, & Luca, 2016). For example, a simple statistical prediction rule (SPR) in a linear model is designed to predict a desired property \( P \) (e.g., future performance) based on a series of cues (e.g., education, experience, and past performance) such that \( P = w_1(c_1) + w_2(c_2) + w_3(c_3) + \ldots + w_n(c_n) \), where \( c_n \) and \( w_n \) reflect the value and weight\(^9\) of the \( n \)th cue (Bishop & Trout, 2005). Research shows that even this simple statistical algorithm is, at least in overall effect, better than humans in hiring predictions, in part because such a hiring algorithm is more consistent than humans (and cheaper, to boot). And, in practice, this algorithm can be better scaled and automated in a consistent way (Chamorro-Premuzic & Akhtar, 2019). Also, the increasing availability of good data, advances in statistical algorithms, and new capacities to analyze large-scale data have made this algorithmic route even more promising (Cappelli, 2020).

Indeed, more advanced statistical hiring algorithms based on machine learning can be better than humans at predicting performance and fit because they are specifically designed to “adaptively use the data to decide how to trade off bias and variance to maximize out-of-sample prediction accuracy” (Chalfin et al., 2016: 124). In this respect, for example, Cowgill (2019) finds that more advanced statistical hiring algorithms based on machine learning better predict job performance than humans because they lack some of the biases from which humans suffer. Also, Chalfin et al. (2016) find that, compared to the existing rank-ordering police hiring

\(^9\) The weight for each cue reflects its importance and is assigned based on the comparison of any given cue to a large set of data on performance (Bishop & Trout, 2005).
systems, machine learning algorithms that use sociodemographic attributes; prior behavior, including prior arrest records; and polygraph results would yield a 4.8 percent reduction in police shootings and physical and verbal abuse complaints.

In addition to the hiring domain, advanced statistical algorithms based on machine learning have been shown to be more effective than humans in a broader set of screening decisions where “a decision-maker must select one or more people from a larger pool on the basis of a prediction of an unknown outcome of interest” (Rambachan, Kleinberg, Ludwig, & Mullainathan, 2020: 91). For example, Kleinberg, Lakkaraju, Leskovec, Ludwig, and Mullainathan (2018) show that machine learning algorithms exhibit better performance than judges in bail decisions because they incorporate fewer irrelevant perceptions of the defendant (e.g., demeanor) into their decisions. Also, Dobbie, Liberman, Paravisini, and Pathania (2018) illustrate that machine learning algorithms minimize bias against certain types of applicants (e.g., immigrants). Other related studies in lending find that machine learning algorithms are better at predicting default (Fuster, Plosser, Schnabl, & Vickery, 2019) and are less discriminatory compared to face-to-face lenders (Bartlett, Morse, Stanton, & Wallace, 2019).

Critics of algorithmic decision-making in hiring (and elsewhere) raise at least two objections. The first objection pertains to the seeming ability of humans to pick up on soft, qualitative, or noncodifiable cues during interviews that are difficult to capture in algorithms (Gigerenzer, 2007; Highhouse, 2008). However, this is precisely where the research shows that there is a high likelihood and magnitude of bias clouding human decision-making. Indeed, the “speculation that humans armed with ‘extra’ qualitative evidence can outperform SPRs has been tested and has failed repeatedly” (Bishop & Trout, 2005: 33). Even if we grant that humans are skilled at inferring relevant information from subtle personality and intellect cues, as some research suggests (Gigerenzer, 2007), statistical algorithms often simply pull on the same cues. While many algorithms tend to draw on codifiable cues (rather than bias-prone, noncodifiable cues), in contrast to humans, algorithms are more efficient and consistent, and they need not be managed with respect to their sense of self-esteem or self-importance (Chamorro-Premuzic & Akhtar, 2019).

The second objection regarding the algorithmic method of predicting future performance and assessing fit concerns fairness (Cappelli, Tambe, & Yakubovich, 2020; Newman, Fast, & Harmon, 2020; Raisch & Krakowski, 2021; Tambe, Cappelli, & Yakubovich, 2019). In this respect, although legitimate fairness concerns are associated with algorithmic predictions of human performance, research has shown that algorithms are often no worse than the alternative means of hiring, including using human judgment through interviews. For example, using data on teacher and police characteristics, Chalfin et al. (2016) show that statistical algorithms predict future performance better than humans. Though there are indeed fairness concerns with algorithms, these concerns are prevalent in human decision-making too (Danieli et al., 2016). Specifically, Danieli et al. grant the prevalence of fairness issues in algorithms but also highlight several comparably concerning psychological biases in human judgment. For example, in hiring contexts, humans engage in bracketing (i.e., overemphasizing subsets of choices over the universe of all
options), that is, choosing the top candidate who was interviewed on a given day instead of the top candidate interviewed throughout the search process (Danieli et al., 2016). In addition, Li (2020) summarizes research that shows how human judgment in hiring may discriminate based on race, religion, national origin, sex, sexual orientation, and age. Given this research, Cappelli (2020) warns us not to romanticize human judgment and to recognize “how disorganized most of our people management practices are now.” He notes, “At least algorithms treat everyone with the same attributes equally, albeit not necessarily fairly.”

Indeed, a significant portion of the algorithmic fairness issues arguably stems from human actions, as well as the lack of diversity in the humans who designed them (Li, 2020) and the types of data with which humans trained them (Cappelli, 2020; De Cremer & De Schutter, 2021). For example, Dastin (2018) reports that Amazon’s recruiting algorithm was biased against women because it was trained to assess candidates by discovering patterns in submitted résumés over a ten-year time frame—most of those résumés were submitted by men (see also Cappelli, 2019a).

As it turns out, recent research challenges the common assumption that biased data in the training stage of machine learning will lead to undesirable social outcomes. Specifically, Rambachan and Roth (2020) empirically examine the “bias in, bias out” assumption and highlight the conditions under which machine learning may reverse bias and ultimately prioritize groups that humans may have marginalized. More specifically, through mathematical modeling and simulation, they show

---

10 What about the possibility of complementing algorithmic predictions with human oversight? In other words, one might be tempted by the thought that a firm should use both algorithms and its own judgment; that is, one should consider the predictions of the algorithms, but vet these predictions against one’s own assessment of the candidate. After all, algorithms will, at least on occasion, offer what seem to be obviously mistaken prescriptions. And if one’s intuition contradicts what the algorithm is prescribing in such a case, one might defect from the algorithmic strategy.

Although tempting, this strategy faces serious problems. A crucial lesson from the literature on how to benefit from SPRs (including decision assistance algorithms) is that partial or selective compliance with the strategy results in significantly worse overall outcomes (Bishop & Trout, 2005; Dawes, Faust, & Meehl, 1989; Meehl, 1957). This has been confirmed on multiple occasions in the laboratory context and is a problem in contexts as wide ranging as medical decision systems and criminal recidivism, as well as in interviews (Bishop & Trout, 2005: 46–47, 91; Goldberg, 1968; Leli & Filskov, 1984; Sawyer, 1966). Specifically, when one opts for a selection strategy based on a SPR (such as an algorithm), but then defects from this strategy on a case by case basis because this particular case seems unique this yields worse overall outcomes (Bishop & Trout, 2005). This is so even if there is a strong sense that the particular circumstance at hand is somehow exceptional (see the literature on the “broken leg problem” [Bishop & Trout, 2005: 45–46; Dawes et al., 1989; Meehl, 1957] when the decision maker “comes to believe she has strong evidence for defecting from the strategy” [Bishop & Trout, 2005: 46]). In other words, to secure the most overall instrumental benefits of an algorithm, its advice generally cannot be taken a la carte.

11 We recognize that, in some instances, algorithms risk amplifying our biases and can further entrench bad organizational cultures (because firms would use their own past HR decisions as data sets, which can in turn deepen morally untoward hiring practices). In such cases, this is indeed a significant added concern with using algorithms in lieu of humans. This, of course, would undermine the strength of our characterization of the algorithmic threat and, in turn, lessen the force of the puzzle we raise for the traditional view of interviewing, but it does not undermine our ultimate thesis that there are strong grounds for preserving the practice of interviewing indeed, this would amount to a further independent consideration that supports our thesis.
that, unlike the bias generated by measurement errors caused by mislabeled data, the bias generated by sample selection may be flipped by machine learning such that the machine learning outcomes would favor groups that encountered discrimination in the training data. Rambachan and Roth argue that the bias reversal occurs because members of groups that are underrepresented in the original training data, for example, women, that make the cut are typically ones that are statistically outstanding performers. As such, in subsequent rounds of learning, the algorithm is fed data in which women are overly positively correlated with being outstanding performers. Rambachan and Roth show that this can ultimately reverse the underrepresentation in the data that is due to human decision makers.

We have thus far considered two objections to using algorithms instead of interviews, and we’ve suggested that these objections fall short. Yet one might correctly point out that many more objections to algorithms have recently appeared in the algorithmic ethics literature (Birhane, 2021; Hunkenschroer & Luetge, 2022; Martin, 2019; Müller, 2021; Tasioulas, 2019; Tsamados et al., 2022). For example, there are concerns related to algorithms systemically excluding certain individuals (Creel & Hellman, 2022), eliciting organizational monocultures (Kleinberg & Raghavan, 2021), or disproportionately harming marginalized groups (Birhane, 2021); worries related to the legitimacy and trustworthiness of algorithms (Benn & Lazr, 2022; Martin & Waldman, 2022; Tong, Jia, Luo, & Fang, 2021) and the lack of explainability in the case of opaque algorithms (Anthony, 2021; Kim & Routledge, 2022; Lu, Lee, Kim, & Danks, 2020; Rahman, 2021; Rudin, 2019; Selbst & Powles, 2017; Vélez, Prunkl, Phillips-Brown, & Lechterman, 2021; Wachter, Mittelstadt, & Floridi, 2017); issues related to whether algorithms preclude us from taking people seriously as individuals (Lippert-Rasmussen, 2011; Susser, 2021); and concerns related to whether automated systems create responsibility or accountability gaps (Bhargava & Velasquez, 2019; Danaher, 2016; Himmelreich, 2019; Nyholm, 2018; Roff, 2013; Simpson & Müller, 2016; Sparrow, 2007; Tigard, 2021), among other concerns (Bedi, 2021; Tasioulas, 2019; Tsamados et al., 2022; Yam & Skorbung, 2021). In short, there’s now a rich literature involving a wide range of concerns related to adopting algorithms in lieu of human decision makers (Hunkenschroer & Luetge, 2022; Martin, 2022; Müller, 2021; Tsamados et al., 2022). And the thought might be put more forcefully: insofar as these two aforementioned concerns could be objections to using algorithms (and in turn objections to the force of the interview puzzle), many more objections—like the ones articulated in the algorithmic ethics literature—may succeed.

We grant the force of this concern. Taken together, the arguments developed in the algorithmic ethics literature constitute a powerful concern regarding using algorithms in lieu of human decision makers. Furthermore, to the extent that these objections to algorithms succeed, it would weaken the strength of the algorithmic

---

12 The algorithm will continue to replicate and exacerbate any bias generated by measurement errors caused by mislabeled data.

13 See also the related debate concerning trade-offs between interpretability and accuracy (London, 2019).

14 We are grateful to an anonymous reviewer for raising this concern.
threat (and, correspondingly, the force of the interview puzzle). However, for our ultimate aims, this does not concern us. This is because our broader project is not to defend algorithms—we do so in the context of the interview puzzle strictly for the sake of argument. Our ultimate aim is instead to argue that even if these wide-ranging objections to the use of algorithms fall short, there nevertheless remain independent moral considerations that tell against abdicating hiring choices to an algorithm. Crucially, the kinds of moral considerations on which we draw do not depend on certain bad outcomes that may arise due to algorithms. This is to say, even if algorithms were not systematically excluding individuals in arbitrary ways (Creel & Hellman, 2022), did not result in an organizational monoculture (Kleinberg & Raghavan, 2021), did not create responsibility gaps (Himmelreich, 2019; Johnson, 2015; Martin, 2019; Matthias, 2004; Roff, 2013; Sparrow, 2007), or did not elicit other morally untoward outcomes, there nevertheless remains an independent moral concern about firms abdicating their choices in the hiring domain to an algorithm. So, the argument we will now provide might be understood as providing further, independent grounds to resist using algorithms (at least in the context of hiring). Moreover, the arguments we offer do not hinge on certain bad outcomes arising due to using algorithms; as such, the force of our arguments remains, even if the bad outcomes associated with algorithms are ultimately engineered away.

2.3 Taking Stock of the Interview Puzzle

The behavioral and algorithmic threats present a significant twofold challenge and raise the interview puzzle for proponents of the traditional view of interviewing. To be sure, this does not mean that the traditional view is not, in part, correct. Finding high-performing candidates who fit the job requirements, as the traditional view posits, is plausibly an important end for firms to pursue. However, the behavioral and algorithmic threats, taken in conjunction, challenge whether interviews are a suitable means toward that end. Crucially, if interviews are only about this end, then the interview puzzle remains and threatens to undermine our justification for conducting interviews. We will now argue, however, that there is more to be said on behalf of interviews than the traditional view accounts for.

Before proceeding, we offer a brief clarification about an assumption we make in the next section: we treat the interview process as equivalent to a hiring process with human decision makers. But, strictly speaking, this assumption is not always correct. Hiring processes with human decision makers can occur without interviews, because interviews are not the only available basis for selection. For example, tests or work samples might instead be used. However, tests and work samples are apt in a much narrower range of positions. Moreover, as HRM textbooks note, “interviews are one of the most common methods used for selection” (Mathis et al., 2016: 259), and “interviews continue to be the primary method companies use to evaluate applicants” (Mondy & Martocchio, 2016: 165). In fact, “while not all employers use tests, it would be very unusual for a manager not to interview a prospective employee” (Dessler, 2020: 192). For these reasons, we use “the interview process” interchangeably with “hiring process conducted by human decision makers.” At the end of section 4, we briefly discuss the implications of relaxing this assumption.
3. THE VALUE OF CHOICE THEORY OF INTERVIEWS

The interview puzzle can be dissolved once we recognize that interviews play additional roles beyond predicting performance and fit. For this reason, even if the behavioral and algorithmic threats undermine the plausibility of interviews serving as a means toward the end of securing an employee who fits the role’s and organization’s needs, we need not conclude that the practice of interviewing is unjustified or something that ought to be abandoned: this is because interviews are a source of other kinds of value and are not exclusively a means for predicting performance and fit.

To be clear, on the view we develop, we do not challenge the importance of the end posited by the traditional view (i.e., the end of hiring an employee who fits the role’s and organization’s needs); rather, we argue that additional kinds of value are implicated in the practice of interviewing. Thus we offer a pluralistic theory of interviewing and argue that once we recognize the wider range of contenders for the kinds of value generated through interviewing, we can see that abandoning interviews would risk the loss of certain important kinds of value.

To understand the additional kinds of value implicated in the practice of interviews, we draw on philosopher T. M. Scanlon’s (1988, 1998) account of the value of choice. Scanlon’s (2013: 12) account “begins from the fact that people often have good reason to want what happens in their lives to depend on the choices they make, that is, on how they respond when presented with the alternatives.” His work on the value of choice has been significant for debates and fields of inquiry as wide-ranging as paternalism (Cornell, 2015), bioethics (Walker, 2022), the freedom and moral responsibility debate (Duus-Otterström, 2011; Fischer, 2008), and contract theory (Dagan, 2019).

On the value of choice account, at least three different kinds of value can be generated when making a choice: instrumental, representative, and symbolic. The first is the instrumental value of a choice: if I am the one who makes the choice, I might make it more likely that I realize some end than were I not given the opportunity to choose. So, for example, if I’m a prospective car buyer and am given the choice over what color I want for my car, my making this choice realizes a certain instrumental value: of making it more likely that the car will satisfy my aesthetic preferences (in contrast to, for example, were the dealership to choose the color of the car on my behalf or were the color to be selected using a random color generator). So, the instrumental value in a choice is realized when it makes it more likely that a desired end of a prospective decision maker is achieved.

The second is the representative value of choice: this is the value that is generated when my making the choice alters the meaning of the outcome of the choice—crucially, this value is realized even if my making the choice is instrumentally worse at achieving certain ends than an alternative method of decision-making (e.g., an algorithm, a coin flip, deference to an expert). For example, it’s important that I am the one who chooses a gift for my partner, not because I’m more likely to satisfy their preferences than they are (were they to choose the gift themselves), but rather because there is value in the fact that I was the one who chose it; in choosing the
gift, I expressed myself (e.g., my desires, beliefs, and attitudes toward my significant other) through that act. More simply, representative value relates to how the outcome of the choice takes on a different meaning in virtue of who makes the choice.

The third is the symbolic value of choice: this is the value associated with certain choices reflecting that one is a competent member of the moral community who has standing that is “normally accorded an adult member of the society” (Scanlon, 1998: 253). For example, if I, as an adult, were not permitted to choose my bedtime, this would be demeaning and infantilizing. This is so even if a sleep specialist choosing my bedtime would result in outcomes better for my circadian rhythm and other physiological markers. My being able to choose reflects the judgment that I am a “competent, independent adult” (Scanlon, 1998: 253). This is the value that is risked when one is denied the opportunity to make certain choices, ones that, in a given social context, are choices that “people are normally expected to make … for themselves” (Scanlon, 1998: 253).

These are the three candidates for the value generated through making a choice. The first is instrumental, and the second two are noninstrumental sources of value. This may not exhaust the candidates for the kinds of value generated in making a choice, but it does taxonomize three important kinds of value that are generated in making a choice. Thus, if a choice is abdicated, (at least) these three kinds of value are at risk and are thus potential candidates for the value that would be lost.

Returning to the context of interviewing, when firms conduct interviews, they are making choices about whom to employ. So, let’s now turn to how the value of choice account bears on interviewing. We will discuss each sort of value generated through choice—instrumental, representative, and symbolic—in turn.

The first is the instrumental value of choice. Securing instrumental value is the chief value with which the traditional view of interviewing is concerned. The thought goes as follows: interviewing realizes the instrumental value to the extent that it helps the firm predict a candidate’s performance and fit. Those who are inclined to preserve interviews, on the basis of the traditional view of interviewing, might expect that the instrumental value of choice realized in interviewing—helping a firm better predict a candidate’s performance and fit—is what both explains why we interview and also what justifies its costs.

Yet the instrumental value of interviewing is precisely what is called into question by the interview puzzle. Interviewing does not excel at generating the purported instrumental value that it is thought to elicit (namely, predicting future performance and fit). So, if the sole kind of value that could be generated through interviewing is instrumental value, then the grounds for the practice are undermined. But as the value of choice account tells us, there is a wider range of contenders for the kinds of value generated in making a choice. The critical oversight of the traditional view is its failure to recognize that the value generated through interviewing is not entirely conditional on the instrumental value of choice, given that there can be noninstrumental value generated through the choice.

This brings us to the second potential value—and one overlooked by the traditional view—that is realized through interviews: the representative value of choice. As Scanlon (1998, 253) points out, we value and want certain choices to “result from...
and hence to reflect [our] own taste, imagination, and powers of discrimination and analysis." In the interview context, we may value the fact that we are the ones choosing with whom we work, and there is value lost (i.e., representative value) when we abdicate that choice, even if our choosing does not as effectively realize the ends of predicting performance and fit as an algorithm. An algorithm might be better at predicting which romantic partner we should date, whom we should befriend, or which university we should attend—while this all might be correct, abdicating these choices and deferring to an algorithm would result in us losing something of value: representative value. Choosing to whom we relate in the workplace is a way “to see features of ourselves manifested in actions and their results” (Scanlon, 1998: 252).

The representative value of a choice is the value that arises in virtue of the choice taking on a different meaning: because of both the fact of who makes the choice and the choice representing or expressing the person’s judgments, desires, and attitudes.

The third value generated through interviewing, and another oversight of the traditional view of interviewing, is the symbolic value of choice. Scanlon (2019: 4) points out, “If it is generally held in one’s society that it is appropriate for people in one’s position to make certain decisions for themselves, then failing to make such a decision for oneself or being denied the opportunity to make it, can be embarrassing, or even humiliating.” Thus the symbolic value of choice is what is lost when a person for whom it would be appropriate (in a given social context) to make a certain decision is precluded from making that decision. For example, to the extent that workplace norms in a given society involve members of an organization typically having a choice in their future colleagues—people with whom they would collaborate but also, in some cases, those whom they would befriend or with whom they would commiserate and form community (Casciaro, 2019; Estlund, 2003; Porter, Woo, Allen, & Keith, 2019)—through interviewing, depriving people of that choice may result in a loss of symbolic value.15 Relatedly, a certain prestige and status are implicated in making certain choices (including selecting future colleagues through interviewing) that figure into the symbolic value of choice; this is especially vivid, for example, when alumni of a university are involved in on-campus recruiting at their alma mater (Binder, Davis, & Bloom, 2015). This prestige and status that are implicated in the symbolic value of choice are also part of what would be lost were firms to forsake interviews. Crucially, substituting interviews with algorithms can result in a loss of symbolic value even if, as a matter of fact, an algorithm may arrive at a better assessment of a candidate’s expected performance and fit.16

For a discussion of the downsides of workplace friendships for organizations, see Pillemer and Rothbard (2018).

It is worth noting that the term algorithm is often used to refer to multiple different kinds of processes, systems, and technologies (Leavitt, Schabram, Hariharan, & Barnes, 2021). For instance, some algorithms are rule based (or symbolic) systems, whereas others are association based systems. Within these broad and rough categories are many varieties of algorithms and ways in which they might be combined and used. For the purposes of our argument, we put to one side the details regarding the technical specifications of algorithms while merely noting that the extent to which a value of choice is undermined by abdicating the choice to an algorithm may also depend on the type and nature of the algorithm.
Although the representative value of choice and the symbolic value of choice may seem similar, especially because, as Scanlon (1998: 253) puts it, “representative and symbolic value may be difficult to distinguish in some cases,” they are not the same. Symbolic value concerns how making certain choices reflects one’s standing, whereas representative value concerns how the meaning of a certain outcome depends on who is making the choice that elicited the outcome. Despite these differences, both are kinds of noninstrumental value, and neither depends on the instrumental effectiveness of the choice with respect to some end (Aristotle, 1962; Donaldson, 2021; Donaldson & Walsh, 2015; Gehman, Treviño, & Garud, 2013; Kant, 2012; O’Neill, 1992; Zimmerman & Bradley, 2019).

Our interviewing practices can be vindicated once we recognize that the choice involved in the interview process can realize both representative and symbolic value. The key point is that “the reasons people have for wanting outcomes to be dependent on their choices often have to do with the significance that this dependence itself has for them, not merely with its efficacy in promoting outcomes that are desirable on other grounds” (Scanlon, 1998: 253). And the fact that representative and symbolic value are threatened when abdicating the choice involved in interviewing a candidate—the choice of whom to relate to in the workplace—generates pro tanto moral reason to preserve interviews as an organizational practice. Crucially, the representative and symbolic value undergirding our interview practices is not imperiled by the behavioral or algorithmic threats.

In other words, once we recognize the broader range of contenders for the kinds of value generated through interviewing, we can see that the behavioral and algorithmic threats only undermine part of the potential value in interviewing—its instrumental value. But we still have pro tanto moral reason to continue the practice of interviewing, given the noninstrumental value—representative and symbolic value—that may be lost were we to abandon the practice.

4. CLARIFICATIONS AND OBJECTIONS

We now turn our attention to a few clarifications and some potential objections. First, it’s worth keeping in mind that even the noninstrumental values in a choice do not always tell in favor of preserving, rather than abdicating, a choice. For example, with respect to representative value, we might prefer, in some circumstances, for our choices not to reflect our judgments, desires, and attitudes. If one’s organization is considering hiring one’s close friend, one might prefer to have the “question of who will get a certain job (whether it will be my friend or some well-qualified stranger) not depend on how I respond when presented with the choice: I want it to be clear that the outcome does not reflect my judgment of their respective merits or my balancing of the competing claims of merit and loyalty” (Scanlon, 1998: 252). In other words, in circumstances that might present a conflict of interest, for example, there might be reasons related to representative value that tell against preserving the choice.

Second, the value of choice is not simply about having a greater number of options from which to select. This is to say, the value of choice generates reasons that “count in favor of ‘having a choice,’ but for reasons of all three kinds having more choice
(over a wider range of alternatives) is not always better than less. Being faced with a wider range of alternatives may simply be distracting, and there are some alternatives it would be better not to have” (Scanlon, 2019: 4). So, in the context of interviewing, we remain agnostic about how the value of choice is affected by having more candidates from whom to select.

Third, one might doubt whether symbolic value would in fact be risked were we to forgo interviews. The point might be pressed as follows: because many (or even most) employees are not involved in hiring decisions, it is not clear that symbolic value would be lost (or that the failure to be involved in the interview process would be demeaning).17 We grant that symbolic value may not be risked in many instances of abdicating a choice. But this clarification points the way to an advantage of our value of choice account: its contextual sensitivity. As Scanlon (1998: 253) notes, a key point with respect to whether symbolic value is risked in a given situation is whether the situation is one “in which people are normally expected to make choices of a certain sort for themselves.” Ascertaining whether there is such an expectation in place in a given hiring context and, in turn, whether symbolic value would be lost will depend on certain sociological facts pertaining to the expectations in the given workplace and the norms governing that workplace culture, field, or industry.18 This means that there is an important role for empiricists to play in ascertaining the workplace contexts, fields, or industries in which symbolic value is risked to a greater or lesser extent. And in contexts in which the strength of the norms associated with choosing members of one’s organization are weaker, the reasons provided by the symbolic value of choice would be correspondingly weaker.

Fourth, one might raise the following question: what about organizations that outsource hiring to an external head-hunting firm? On our view, such an approach would, in effect, be morally akin to abdicating the choice to an algorithm, with respect to the value of choice. That said, there might be other sorts of considerations—for example, the various objections discussed in the algorithmic ethics literature

17 We are grateful to an anonymous reviewer for this point. We also acknowledge that many hiring decisions are made by internal HR divisions. But it is worth noting that even if these members of HR divisions may not ultimately work with the people they are hiring (unless, of course, the interview is for an HR position), the members of these HR divisions are themselves usually employees of the organization too. Moreover, in a number of fields, it is not uncommon in the final rounds of interviews for candidates to be interviewed by individuals who would be their immediate team members and managers if selected for the position.

18 Suppose a firm is deciding on candidates as a collective by using some sort of majoritarian procedure that nevertheless results in an outcome that is no individual’s most preferred choice (List & Pettit, 2011; Pettit, 2007). First, does the individual’s choice still matter? Our aim here in this article is not to enter the debate regarding the metaphysics and morality of group agents. That said, we note that the value of choice of the individual still matters, given that it is a key component of fixing the collective’s choice. It is quite unlike cases in which an individual’s choice (arguably) may not matter due to an outcome being causally overde terminated. That an individual’s most preferred choice was not instantiated is a different matter from the value realized through making the choice. Second, such a collective decision procedure seems morally unobjectionable—could automating it render it objectionable? It may very well, albeit perhaps not for reasons related to the value of choice. This is because automating a procedure can change its very nature, morally speaking, for reasons of the sort discussed in the algorithmic ethics literature. We are grateful to an anonymous reviewer for these two questions.
mentioned earlier—that make relying on algorithms morally worse than abdicating the choice to an external head-hunting firm. Still, it is quite right that the value of choice-related considerations would be morally akin. But this need not mean that there is no role for external head-hunting firms at all. This is because the concerns with respect to the value of choice primarily arise insofar as the firm defers to the judgment of the external head-hunting firm. This, however, does not preclude soliciting advice about hiring decisions from HR consultants or head-hunting firms. Notably, in the context of algorithms, deference to the algorithm is much more likely given that many algorithms are opaque. Moreover, failing to defer to the judgments of the algorithm—that is, picking and choosing on a case-by-case basis when to follow its prescriptions—drastically undercuts its overall instrumental benefits (Bishop & Trout, 2005).

Fifth, perhaps, all things considered, in some instances the costs of interviewing may be too burdensome and a firm might be forced to forgo the practice. Perhaps, in other instances, the importance of finding the right person is far too weighty—for example, selecting an airline pilot—for a human to make the decision if an algorithm would do so more effectively. But even in these cases, were we to abandon interviewing for a different selection method (e.g., an algorithm), it’s worth keeping in mind that there may still be something of normative significance lost, that is, representative or symbolic value.19

How might these trade-offs be managed? One potential approach might be as follows: suppose one regards instrumental value to be of much greater significance in the business realm than the sorts of noninstrumental value to which we’ve drawn attention. In such a case, a hybrid approach might be considered. Such an approach might involve conducting the initial screening with an algorithm and leaving the ultimate decision to a member of the organization. This may allow for reducing the potential trade-offs between the instrumental and the noninstrumental sources of value of choice.20

In other words, our view is not that, in instances when an algorithm is vastly superior at achieving a given end, firms should pursue the drastically less instrumentally effective approach. As Scanlon (2019: 4) notes, the various reasons for the value of choice “can conflict with reasons of other kinds, particularly with instrumental reasons.” So, we are not claiming that firms must always conduct interviews, instead of using algorithms. Nor are we claiming that the instrumental considerations are not of moral significance—in some instances, they may very well be of overriding moral importance.21 Rather, our point is that multiple kinds of value can be

19 Quite apart from the representative or symbolic value that is risked when abdicating a choice to an algorithm are concerns about how doing so might undermine organizational learning (Balasubramanian, Ye, & Xu, 2022).

20 Of course, as earlier noted, picking and choosing when to comply with the predictions of the algorithm significantly undercuts the overall instrumental benefits of the algorithm (Bishop & Trout, 2005). Insofar as one pursues such a hybrid approach, it’s worth keeping in mind that the various other moral objections to the use of algorithms discussed in the algorithmic ethics literature would still be relevant.

21 Suppose a physician faces two options: interpret medical images herself or rely on a predictive algorithm. Further suppose that the algorithm yields better instrumental results with respect to patient welfare.
generated through the practice of interviewing—including sources of value that may generate conflicting reasons—and that an adequate theory of interviewing should not overlook this fact. If we are to abdicate interviews in a given context, we should do so in full view of the kinds of value that are risked.22

Sixth, it’s now worth revisiting the assumption we articulated at the end of section 2: treating the interview process as equivalent to a hiring process with human decision makers. As we acknowledged, this assumption is not always, strictly speaking, correct. A hiring process—including one in which humans are making the decisions—might not involve interviews at all; perhaps the hiring process involves choosing on the basis of work samples or tests.

So, when we relax this assumption, what follows? Our view would still imply that abdicating the hiring process entirely to algorithms would risk the various values of choice. However, our value of choice account does not entail a particular mode of choosing for a human decision maker—whether interviews, work samples, or tests. With respect to the narrow range of professions where work samples or tests can aptly be implemented, our value of choice arguments are neutral between choosing such an approach and interviewing (but of course, the value of choice account is not neutral between either of these routes and abdicating the choice to an algorithm).23

Interviews are a way—the most prominent and common way, and the way most broadly applicable across a range of positions—for us to choose the members of our organizations, but they are indeed not the only way to choose in the hiring process.

To summarize, we have offered an account of some heretofore underappreciated normative dimensions of a widespread business practice, namely, interviewing. Our view helps address some of the challenges to which the traditional conception of interviewing succumbs. The traditional view has difficulty explaining why interviews persist and justifying why we should not abandon them, given their costs, our poor ability to predict performance and fit, and the presence of algorithmic alternatives. Our value of choice theory of interviewing both explains why interviews persist and justifies why there are grounds not to abandon the practice: interviews

---

22 Our argument is neither about the badness of having fewer choices to make nor about the goodness of having more choices to make (nor is it about preserving the status quo number of choices one makes). With respect to the value of choice, that some other choice is made (e.g., to defer to an algorithm) has little bearing on whether, what kind, and the extent to which one of the values of choice would be undermined in abdicating this choice. Adding a choice elsewhere doesn’t somehow replenish the value of choice that is undermined in no longer choosing one’s colleagues.

23 Of course, the various ways in which we are bad at interviewing characterized in the behavioral threat section might tell in favor of choosing by way of these alternative modes of selection (e.g., tests or work samples) when possible. But we hesitate to make this judgment with confidence, given that different kinds of normative concerns may be associated with relying strictly on work samples or tests; for example, it potentially reduces people to a contrived and narrow set of criteria, rather than treating them with respect as individuals and as fellow members of the moral community. For an additional approach to hiring, see Sterling and Merluzzi’s (2019) exploration of “tryouts” and their theoretical and practical potential.
play an important normative function by securing noninstrumental sources of value in hiring.

5. FUTURE AVENUES OF RESEARCH

Our value of choice account of interviewing suggests several new avenues of research. First, a significant body of research in employment ethics primarily emphasizes the ethics of how employers ought to treat their employees (Arnold, 2010; Barry, 2007; Bhargava, 2020; Brennan, 2019; McCall, 2003; Werhane, Radin, & Bowie, 2004), but there is much less, apart from discrimination-related issues, surrounding the ethics of what is owed to prospective employees. Our work highlights the significance of a range of understudied issues to explore in this domain. Although some have explored the question of what is owed to former employees of a firm (Kim, 2014), what, if at all, is owed to potential employees, such as candidates who participate in interviews? Other such issues include, for example, the ethics of exploding offers, accepting applications from candidates that will never be considered, and alerting candidates of rejection. On the side of the candidate, issues include the ethics of feigning enthusiasm for an interview, pursuing an interview merely to solicit an external offer for negotiation leverage, and holding on to offers that one is confident one will not accept.

Second, our account of interviewing points the way to questions related to what may make employment relationships meaningful (Robertson, O’Reilly, & Hannah, 2020). Some contributors to the future of work scholarly conversation have argued that employers owe it to their employees to provide meaningful work (Bowie, 1998; Kim & Scheller-Wolf, 2019; Michaelson, 2021; Veltman, 2016). By attending to the broader range of values associated with interviewing, managers may have the opportunity to make work and employment relationships more meaningful (Bartel, Wrzesniewski, & Wiesenfeld, 2012; Freeman, Harrison, Wicks, Parmar, & De Colle, 2010; Rosso, Dekas, & Wrzesniewski, 2010). So, an important question to address will be how the process of being selected for a position (i.e., through an interview or through selection by way of an algorithm) can contribute to preserving or promoting the meaningfulness of work (Carton, 2018; Grant, 2012; Jiang, 2021; Kim, Sezer, Schroeder, Risen, Gino, & Norton, 2021; Rauch & Ansari, 2022).

Third, there is a sense in which using algorithms in hiring decisions deepens the informational asymmetry between candidates and employers (Curchod, Patriotta, Cohen, & Neysen, 2020; Yam & Skorburg, 2021: 614). Switching to algorithms in hiring may prevent candidates from developing a better understanding of their prospective colleagues and the prospective employer’s workplace culture and norms. On the other hand, if an interview was conducted, the candidate might have acquired this sort of valuable information, even if fallibly. Future scholars should explore the public policy implications of forgoing interviews, especially in jurisdictions with employment at will. The symmetrical right to exit is sometimes discussed as a potential justification for employment at will (Bhargava & Young, 2022;
Hirschman, 1970; Maitland, 1989; Taylor, 2017). But when candidates and employers enter the employment relationship on starkly asymmetric informational grounds (Caulfield, 2021), it’s worth exploring whether the fact of both parties having a right to exit the relationship loses some of its justificatory force with respect to employment at will and considering whether supplementary regulatory constraints would be in order.

6. CONCLUSION

The traditional view of interviewing espoused by both practitioners and management scholars alike holds that interviews are conducted—despite the steep costs associated with the process—to predict a candidate’s performance and fit in relation to a vacancy. We argue that the traditional view faces a twofold threat: the behavioral and the algorithmic threats. The behavioral threat arises in virtue of a large body of behavioral evidence that points to us being poor predictors of future performance and bad judges of fit. The algorithmic threat arises in virtue of algorithms already being superior predictors of performance and fit than us in a number of domains, including the hiring domain.

If the traditional view of interviewing captures all there is to interviewing, then the justification for conducting interviews is undermined by the behavioral and algorithmic threats. However, we argue that the practice of interviewing can be vindicated once we recognize that there are a broader range of contenders for the kinds of value that can be realized through interviewing—crucially, some of these kinds of noninstrumental value that are realized through interviewing remain insulated from the behavioral and algorithmic threats. In short, we argue that even if algorithms are better predictors of performance and fit than us, it does not follow that we ought to abandon our interview practices: this is because important kinds of noninstrumental value are generated through interviewing that could be lost were we to forgo the practice.

Acknowledgments

The authors contributed equally. For helpful comments, feedback, or conversation, we thank Alan Strudler, Ben Bronner, Carson Young, Esther Sackett, Gui Carvalho, JR Keller, Julian Dreiman, Matthew Bidwell, Matthew Caulfield, Peter Cappelli, Robert Prentice, Samuel Mortimer, Sonu Bedi, Suneal Bedi, Thomas Choate, Thomas Donaldson, and audiences at the 2019 Summer Stakeholder Seminar at the University of Virginia’s Darden School of Business, the 2021 Society for Business Ethics meeting, Georgetown Institute for the Study of Markets and Ethics, and the Dartmouth Ethics Institute. We also are grateful to associate editor Jeffrey Moriarty and three anonymous reviewers for their helpful feedback.

REFERENCES


https://doi.org/10.1017/beq.2022.41 Published online by Cambridge University Press


Vikram R. Bhargava (vrb@gwu.edu, corresponding author) is an assistant professor of strategic management and public policy at the George Washington University School of Business. He received a joint PhD from the University of Pennsylvania’s Wharton School and Department of Philosophy.

Pooria Assadi is an assistant professor of management and organizations in the College of Business at California State University, Sacramento. He received his PhD in strategic management from Simon Fraser University’s Beedie School of Business and was a visiting scholar at the University of Pennsylvania’s Wharton School.

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.
Hi (b)(6) PII

I am very concerned of disability tracking because of what happened to me when I was working at my previous job (b)(6) PII. When I was working (b)(6) PII in Harrisburg and they relocated their warehouse to Camp Hill, the work staff laid me off because they thought the job was not a good enough fit for me just because I was I was blind! I was livid! I couldn’t believe it! I literally was having trouble with staying a happy person after that! One day: I was so unhappy that I called them up and told them something about myself and threatened to do something upsetting to myself that would have had severe consequences! But then I regretted that slip immediately. For they told me they were going to report it to the job counselor and they did. Meanwhile: (b) (6) and told her what happened. She said that it was their job to report that kind of stuff but she was glad that I reached out to her after what happened. The next day: I called my job counselor and told her that I was sorry for what happened about the phone call. I told her that I really didn’t mean it and she said that she understood and that it was just that I was dealing with a lot of frustration. I am worried that if automated disability tracking technology were to be installed in (b)(6) PII and not enough information about me or other workers with blindness ever come in there is known then the same thing will happen to me (b)(6) PII So please let this story be a lesson to all of those who want to work and are blind or maybe have another disability that may put them at risk of losing their job sent from my iPhonev
I'm a FedEx Express Driver. FedEx installed Cameras in the Cabs of our Vehicles a couple years ago.

Each Employee had to sign into a Corporate Mandated Acknowledgement site to agree to be recorded if wanted to be an Employee of the Company.

It records if eyes are not on the road, if we are on our cell phones while driving, if using our FedEx equipment. It must track our eye movements, because i've noticed if i'm wearing Sunglasses…it does not beep as much.

From what i understand, our Operation Managers get email notifications (can access the recordings) for each Camera Notification. Multiple violations and/or any serious violations and we are required to get a Check-Ride or Documented discipline.

We are all kind of used to it now…but it is very invasive and strange.

Corporate is selling it as a “Safety” implementation.

Thank you,
Adam

Sent from Yahoo Mail for iPhone
Regarding: Automated Worker Surveillance and Management

As an investment consultant focused on private equity, my written communication is constantly monitored by my employer. This surveillance is not disclosed. Employees are denied knowledge of the specific mechanisms of how this is happening.

The ability of a bad actor or employer to right now access my written communication, without informed consent or ability to escape, has a chilling effect on reaching out for help internally and externally. The automated, continuous, and unspecified collection of written communication also renders employees vulnerable to retaliation, stochastic harassment, and unfair dismissal.

This industry is captive to their own’s economic self-interest and unwilling to acknowledge how surveillance is being misused to cut down the few protections available to employees. As a recent example, surveillance was used by an employer to game the National Labor Relations Board (NLRB) protection of employees: surveilled written communications assessed the likelihood an employee would reach out to agencies like the NLRB, then the employer pro-actively managed employee titles/responsibilities to ring fence their own liability.

The red flag, from my perspective, is that this misuse of surveillance is currently not illegal, not considered morally unconscionable, and is not economically punitive. If C-suite executives, with tacit approval from their boards, can continue this cruel demonstration of surveillance as a tactic to limit liability, then we are leaving in place the rationale for this terrifying form of surveillance to proliferate. I hope the White House Office of Science and Technology Policy’s request for information will increase the cost of misusing surveillance technology and help protect employees and their family’s basic fundamental rights to privacy and human dignity.

Best regards,

Sean Castillo
Hello:

I have worked for a facility for many years, including working from home. I have felt that my employer has been using software monitoring tools to distract me while I am doing my work on their work computer. They can make changes to the connection in Citrix where we get access to use our programs and the software Epic Hyperspace and Extract have been slow and can be hard to type. I also have seen software changes that don’t happen on other work computers at the office. from all this and worrying over my job performance for years plus submitting multiple IT tickets (HR also asked me to re-image the hard drive but I started having the same issues in less than a week later). I also have a workplace accommodation. Even before workplace accommodation approved, they can see from how I work that I am easily distracted and forgetful and I need to re-check my work before submitting my work to be checked by our quality check coordinator. They can also disable features that I need to see what I am doing correctly; the program should stop and allow me to review but I have received errors where I can’t go back and correct my mistakes. I’m afraid I’m going to lose my current position with my employer.

-Christina Raley

Sent from my iPhone 14
Hello, my name is Matt Muscarnera.

First of all thank you for creating this feedback request so we can provide information on surveillance tactics currently ongoing by companies. I work for State Farm who currently has almost harassing levels of surveillance. As soon as you log into work everything you do is tracked. If you do not move your mouse for 90 seconds you're immediately considered as idle even if you are currently assisting a customer. It's to the point where managers encourage you to move your mouse randomly just so you don't get considered as idle. Every thing you do in claims is tracked and calculated. How you serve the customer does not matter as long as your numbers are good. Their level of surveillance does not encourage growth or for anyone to perform above what they are asked. Instead it makes people get just their numbers and focus on not getting any lists for a surveillance tracker going off, such as too much idle time. You must be on camera during any meeting on teams.
In responding to the White House RFI on workers surveillance I write to give a couple of examples that have pushed in the construction field. First is the time keeping apps that employers are trying to force employees to put on their personal phones for recording time. It shows thru GPS coordinates where an employee is during their non compensated time. They are also requiring that people be on site of the project in their GPS to log in which subsequently also is requiring them to clock out when they leave a jobsite. This becomes an issue when an employee is traveling between jobsites or in a company vehicle that is carrying tools to a jobsite or between jobsites. Both of those situations require compensation per our CBA’s and also under state law because they are under the direction of the employer and driving company equipment to get company tools that are required/necessary to be used on the job.

A second example is several companies are putting inward facing cameras in their company owned equipment and vehicles. This is because of insurance reasons primarily I believe but it records every action, facial expression word and interaction happening in the equipment or vehicle. This means they are under constant recorded surveillance in the employment of their jobs if they are drivers or operating equipment in some situations.

The third example I have is call the Triax system. There were facilities that were trying to force the Triax system on our construction workers. Specifically, it was a healthcare/hospital that was trying to implement this across all employees. Their excuse was security in that they needed to know where everyone was at all times when they were in their facility for security reasons. However, they would not agree that the system would be used exclusively for that purpose and put in writing it would not be used for punitive or negative consequences so we at the local bldg. trades level fought back on its implementation. The Triax system recording height from the ground ie.. if you were on a ladder. Could alert the system if you did not move for a preset amount of time. ie.. potentially being non productive. The facility was also not proposing to track all of their employees just the construction workers remodeling the facility and any one else they wanted to track movements of.

These are the basics of the three different examples I have besides the regular putting GPS trackers on their company vehicles and equipment which is pretty common for anti theft reasons as well as making sure employees are not at the bars with the company vehicles.

Fraternally,

Joe Fowler
Business Manager
Laborers Local 563
June 15, 2023

Deirdre Mulligan, Deputy U.S. Chief Technology Officer for Policy
Alan Mislove, Assistant Director for Data and Democracy
White House Office of Science and Technology Policy (OSTP)

Jenny Yang, Deputy Assistant to the President for Racial Justice and Equity
White House Domestic Policy Council

RE: Request for Information; The Biden Administration and Members of Congress Are Increasingly Encouraging Surveillance, Management, and Exclusion of Workers with Actual and Perceived Mental Health Conditions and Disabilities

Dear Hon. Deirdre Mulligan, Alan Mislove, and Jenny Yang:

I write in my individual capacity in response to your request for information with the observation that surveillance and management of individuals with actual or perceived mental health conditions and disabilities has become ubiquitous, particularly in schools (see APPENDIX I) and the workplace. Such surveillance in the workplace is in fact explicitly encouraged in Sections 2703-2705 of the American Rescue Plan Act of 2021, the Dr. Lorna Breen Health Care Provider Protection Act of 2022, the Supporting the Mental Health of Educators and Staff Act of 2023, and the Providing Resources and Occupational Training for Emotional Crisis and Trauma

2 See, e.g., American Rescue Plan Act of 2021, Pub. L. No. 117-2, § 2704, 135 Stat. 4, 46 (2021) (appropriating $20,000,000 for FY 2021 for the HHS Secretary and CDC Director, “in consultation with the medical professional community” “to carry out a national evidence based education and awareness campaign directed at health care professionals and first responders (such as emergency medical service providers), and employers of such professionals and first responders. Such awareness campaign shall— (1) encourage primary prevention of mental health conditions and substance use disorders and secondary and tertiary prevention by encouraging health care professionals to seek support and treatment for their own mental health and substance use concerns; and (2) help such professionals to identify risk factors in themselves and others and respond to such risks”)
3 Dr. Lorna Breen Health Care Provider Protection Act, Pub. L. No. 117–105, § 3–4, 136 Stat. 1118, 1118-19 (2022) (codified at 42 U.S.C. § 2941) (“improving awareness among health care professionals about risk factors for, and signs of, suicide and mental health or substance use disorders”; “encourage health care professionals to seek support and care for their mental health or substance use concerns, to help such professionals identify risk factors associated with suicide and mental health conditions, and to help such professionals learn how best to respond to such risks”)
4 Supporting the Mental Health of Educators and Staff Act of 2023, H.R. 744, 118th Cong. § 3 (1st Sess. 2023) (“in consultation with relevant stakeholders, including medical professional associations, shall establish a national
It is explicitly encouraged by subagencies of the U.S. Department of Health and Human Services (HHS),7 the Surgeon General,8 and the U.S. Department of Labor’s (DOL) Office of Disability Employment Policy (ODEP),9 and in institutional policies, such as those promulgated

evidence-based or evidence-informed education and awareness initiative—(1) to encourage education professionals and other school staff to seek support and care for their mental health or substance use concerns, to help such professionals and staff identify factors associated with risks for suicide and mental health conditions, and to help such professionals and staff learn how best to respond to such risks”)
5 Providing Resources and Occupational Training for Emotional Crisis and Trauma (PROTECT) in 911 Act, H.R. 2763, 118th Cong. § 2 (1st Sess. 2023) (“To require the Secretary of Health and Human Services to improve the detection, prevention, and treatment of mental health issues among public safety telecommunicators”; “develop and make publicly available evidence-based best practices to identify, prevent, and treat posttraumatic stress disorder and co-occurring disorders in public safety telecommunicators”)
6 DHS Suicide Prevention and Resiliency for Law Enforcement Act, S. 1137, 118th Cong. § 2 (1st Sess. 2023); DHS Suicide Prevention and Resiliency for Law Enforcement Act, H.R. 2577, 118th Cong. § 2 (1st Sess. 2023) (“conduct data collection and research on mental health, suicides, and, to the extent possible, attempted suicides, of law enforcement personnel within the Department of Homeland Security”; “promote education and training related to mental health, resilience, suicide prevention, stigma, and mental health resources to raise mental health awareness and to support others the needs of supervisors, clinicians, care-givers, peer support members, chaplains, and those who have been exposed to trauma”; “promote a culture that reduces the stigma of seeking mental health assistance through regular messaging, training, and raising mental health awareness”)
7 See, e.g., CTS. FOR DISEASE CONTROL & PREVENTION, MENTAL HEALTH IN THE WORKPLACE: MENTAL HEALTH DISORDERS AND STRESS AFFECT WORKING-AGE AMERICANS 3, 5 (July 2018),
9 Office of Disability Emp’t Policy, U.S. Dep’t of Labor, Mental Health: Employers,
https://www.dol.gov/agencies/odep/program-areas/mental-health/employers (last visited May 23, 2023) directs employers to NAT’L ALLIANCE ON MENTAL ILLNESS (NAMI)—NYC METRO, NE. BUS. GROUP ON HEALTH (NEBGH), P’SHIP FOR WORKPLACE MENTAL HEALTH/AM. PSYCHIATRIC ASS’N FOUND.,
PRICEnthouseCOOPERS, & THE KENNEDY FORuM, WORKING WELL: LEADING A MENTALLY HEALTHY BUSINESS 12, 17, 22-23 (June 2016), https://www.psychiatry.org/File%20Library/PWMH.working-well-toolkit.pdf (“[t]rain leaders to identify emotional distress and refer to [employee assistance program] EAP or other behavioral health resources”; “give employees and managers the knowledge and tools to recognize depression and intervene at an early stage to help affected colleagues”; “[p]rovide training in identifying job performance problems related to mental health issues,” “[p]rovide Health Risk Appraisals (HRA) to employees that include mental health questions and questions about management and supervisor support for team member health. Include questions related to stress, depression, and substance use disorders in health risk appraisals”; “Provide information and EAP to those who screen positive. Consider having EAP reach out to positive screens rather than relying on the individual to follow up”) and to Right Direction for Me, Presentation for Manager Training for Right Direction,
by the American Medical Association (AMA) (see APPENDIX II) and the Accreditation Council for Graduate Medical Education10 (ACGME) (see APPENDIX III). The provisions of the Stop Spying Bosses Act prohibiting collection of information on health status, health conditions, and disability status,11 while a step in the right direction, are grossly inadequate to stop spying bosses from engaging in surveillance of workers with actual and perceived mental health conditions and disabilities.

As surveillance of workers with actual or perceived mental health conditions and disabilities has increasingly become condoned and encouraged, employers need not conduct such surveillance surreptitiously or via electronic means, and this surveillance still takes the form of in-person medical inquiries and examinations. I argue that this in-person surveillance is at least as problematic as electronic surveillance, will lead to electronic systems of surveillance in the future, and is a major cause of the exclusion of individuals with mental health conditions and disabilities from the workforce.

My recommendations include formally repealing legislation or at least no longer funding federal programs that encourage surveillance and management of individuals with mental health conditions and disabilities (including those listed in APPENDIX I). They also include directing federal government agencies, including the U.S. HHS, Surgeon General, and ODEP, to stop encouraging this surveillance. Finally, I recommend that the Biden administration direct the U.S. Equal Employment Opportunity Commission (EEOC) to include disabled and LGBTQ+ individuals on its EEO forms; direct the DOL’s Office of Federal Contract Compliance Programs (OFCCP) to update its disability affirmative action regulations under Section 503 of the Rehabilitation Act for federal contractors to align with the EEOC’s disability affirmative action regulations under Section 501 of the Rehabilitation Act for federal employment; and to include persons with disabilities within health workforce inclusion statutes.

These changes are needed to transform an administration and Congressional agenda that appears intent on surveillance and excluding individuals with mental health conditions and disabilities, to one of inclusion. They are needed because of an administration and Congress that diagnostic criteria (e.g., “Feelings of sadness,” and “Sleep disturbance”), and also making unfounded claims that “signs” of depression include “[p]oor quality work,” [p]rocrastination, accidents on the job,” “[i]ndecisiveness, slowed productivity,” “[p]resenteeism—‘just showing up,’” “[m]issed deadlines, absenteeism,” “[p]oor relationships with co-workers, a boss, clients,” “[l]ow morale,” and “[l]ate to work.”

10 Accreditation Council for Graduate Med. Educ. (ACGME), Common Program Requirements 46, https://www.acgme.org/globalassets/pfassets/programrequirements/cprresidency_2022v3.pdf (asking “residents and faculty members to alert the program director or other designated personnel or programs when they are concerned that another resident, fellow, or faculty member may be displaying signs of burnout, depression, a substance use disorder.”)

11 Stop Spying Bosses Act, S. 262, 118th Cong. § 4 (1st Sess. 2023) (“An employer, or, as applicable, a third party or service provider that the employer uses for workplace surveillance may not … except as otherwise provided in law, collect information on or identify the health status, any health condition, or disability status of a covered individual, that is unrelated to the performance of the job duties of the covered individual for the employer”). Employers would most likely circumvent this provision (1) by claiming that workers’ health status, health conditions, or disability status are always related to the performance of the any job duties; (2) by claiming that they are collecting this information not for the purpose of “us[ing] workplace surveillance” but rather for the purpose of developing health interventions that will enhance workers’ performance of job duties; (3) by citing laws purported to allow them to collect this information.
seem to “care” quite a lot about our “mental health,” but not about people with mental health conditions. That “care” very much about optimizing our “mental health” and preventing it from allegedly posing safety threats, but not at all about including people with mental health conditions and disabilities.

TABLE OF CONTENTS

INTRODUCTION

A. SURVEILLANCE OF PEOPLE WITH MENTAL HEALTH CONDITIONS AND DISABILITIES HAS BECOME UBIQUITOUS

B. THE EXCLUSION OF INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES FROM THE WORKPLACE

C. THE SURVEILLANCE OF PEOPLE WITH MENTAL HEALTH CONDITIONS AND DISABILITIES IS A CAUSE OF THEIR EXCLUSION FROM THE WORKFORCE

D. IN-PERSON SURVEILLANCE OF WORKERS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES IS AT LEAST AS PROBLEMATIC AS ELECTRONIC SURVEILLANCE, LEADS TO ELECTRONIC SURVEILLANCE, AND ENHANCES ITS DISCRIMINATORY EFFECTS

I. A DESCRIPTION OF SURVEILLANCE AND MANAGEMENT OF STUDENTS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

A. PROMOTED IN FEDERAL GRANT PROGRAMS

B. PROMOTED IN FEDERAL STATUTES

II. A DESCRIPTION OF SURVEILLANCE AND MANAGEMENT OF WORKERS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

A. PROMOTED BY THE U.S. HHS AND ODEP

B. PROMOTED IN RECENT AND PROPOSED FEDERAL LEGISLATION SINCE 2021

C. WHY THESE AWARENESS ACTIVITIES UNDERMINE THE SPIRIT IF NOT THE LETTER OF THE LAWS PROHIBITING MEDICAL (DISABILITY-RELATED) INQUIRIES OF CURRENT EMPLOYEES UNDER THE ADA

1. THE PURPOSE OF THE ADA’S PROHIBITIONS ON DISABILITY-RELATED INQUIRIES OF CURRENT EMPLOYEES
(a) Why Privacy Protections for Current Employees with Mental Health Conditions Are Particularly Important

(b) Privacy Protections Preempt Employment Discrimination Before It Occurs and Offer Other Antidiscrimination Advantages

2. WHY THE AWARENESS ACTIVITIES ENCOURAGED BY THE U.S. HHS, ODEP, AND FEDERAL LEGISLATION SINCE 2021, UNDERMINE ADA PROHIBITIONS ON DISABILITY-RELATED INQUIRIES

(a) Disability-Related?

(b) Disability-Related Inquiry?

(c) Disability-Related Inquiry by Employer?

III. IT IS PREMATURE TO TURN ATTENTION AWAY FROM IN-PERSON SURVEILLANCE OF WORKERS THROUGH MEDICAL (DISABILITY-RELATED) INQUIRIES AND EXAMINATIONS

A. EXPLAINING PROGRESSIVE CONCERNS WITH ELECTRONIC SURVEILLANCE OF WORKERS, BUT NOT WITH MEDICAL (DISABILITY-RELATED) INQUIRIES/EXAMINATIONS, AND WHY THE LATER REPRESENT AN OVERLOOKED THREAT

1. RISE OF EAP/WELLNESS PERSONNEL IN THE WORKPLACE

2. GREATER INTRINSIC PRIVACY, DIGNITARY HARMS OF DISABILITY-RELATED INQUIRIES/EXAMINATIONS

3. MORE PATERNALISTIC JUSTIFICATIONS FOR DISABILITY-RELATED INQUIRIES/EXAMINATIONS

4. RECENT GOVERNMENT SUPPORT FOR SURVEILLING INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES THROUGH DISABILITY-RELATED INQUIRIES AND WHY THE RESULTING DATA COLLECTED WILL RESULT IN ELECTRONIC, AUTOMATED WORKER SURVEILLANCE AND MANAGEMENT

B. SELECT MEDICAL (DISABILITY-RELATED) INQUIRY/EXAMINATION CASE HISTORY AND DISCUSSION OF THEIR FUNCTIONS

1. FUNCTIONING TO SUPPRESS DISCRIMINATION AND RETALIATION CLAIMS

2. FUNCTIONING TO CONTROL WOMEN AND THEIR PRIVATE SEXUAL LIVES

3. FUNCTIONING OTHERWISE TO JUSTIFY CONTROL AND ADVERSE EMPLOYMENT ACTIONS AGAINST WORKERS UNDER THE GUISE OF PATERNALISM AND CARING

4. FUNCTIONING FOR MORE OBVIOUSLY OVERT PUNITIVE AND MALICIOUS PURPOSES

5. FUNCTIONING TO COLLECT DATA, CREATE ALGORITHMIC WORKPLACE DISCRIMINATION TOOLS, AND FACILITATE AGE/DISABILITY DISCRIMINATION—EEOC v. YALE NEW HAVEN HOSPITAL, INC
IV. RESPONSES TO SPECIFIC REQUEST FOR INFORMATION QUESTIONS

V. RECOMMENDATIONS

A. REPEAL OR AT LEAST STOP FUNDING FEDERAL GRANT PROGRAMS THAT ENCOURAGE SURVEILLANCE AND MANAGEMENT OF INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

B. DIRECT FEDERAL GOVERNMENT AGENCIES, INCLUDING THE U.S. HHS, SURGEON GENERAL, AND ODEP, TO STOP ENCOURAGING SURVEILLANCE AND MANAGEMENT OF INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

C. DIRECT THE HHS OFFICE OF HUMAN RESEARCH PROTECTIONS TO ISSUE APPROPRIATE GUIDANCE; DO NOT FUND FEDERAL RESEARCH AT INSTITUTIONS THAT ENGAGE IN MEDICAL RESEARCH, INQUIRIES, OR EXAMINATIONS OF EMPLOYEES

D. INCLUDE PEOPLE WITH DISABILITIES IN HEALTH WORKFORCE INCLUSION STATUTES; ADD DISABILITIES TO THE EEOC’S EEO FORMS; UPDATE SECTION 503 TO ALIGN WITH SECTION 501

APPENDIX I. SECTIONS OF THE U.S.C. AUTHORIZING OR CONTRIBUTING TO MENTAL AND BEHAVIORAL HEALTH SURVEILLANCE IN SCHOOLS

APPENDIX II. AMERICAN MEDICAL ASSOCIATION (AMA) POLICIES

APPENDIX III. ACCREDITATION COUNCIL FOR GRADUATE MEDICAL EDUCATION (ACGME) COMMON PROGRAM REQUIREMENTS
INTRODUCTION

A. SURVEILLANCE OF PEOPLE WITH MENTAL HEALTH CONDITIONS AND DISABILITIES HAS BECOME UBIQUITOUS

It has become increasingly encouraged by administrations and Members of Congress from both parties. As the Center for American Progress observed in 2019, “[i]nstead of protecting the rights of people with mental health disabilities, lawmakers are using the growing urgency around gun violence as a pretext to expand surveillance and criminalization.”12 At the same time, most news stories on persons with mental health conditions have continued to mention violence,13 and public “perceptions regarding potential violence [from people with mental illness] and support for coercion generally rose” over the last 20 years14—even though persons with severe mental illness have the same chances of being violent as any other person in the general population.15 In this context, it is not surprising that mental health surveillance has become ubiquitous over the last 20 years across society, particularly in schools and workplaces.

B. THE EXCLUSION OF INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES FROM THE WORKPLACE

It should also not be surprising that persons with mental health conditions and disabilities are almost completely excluded from federal government and policy leadership. Persons with the psychiatric disabilities of major depression, bipolar disorder, schizophrenia, posttraumatic stress

12 Azza Altiraifi & Valerie Novack, Efforts to Address Gun Violence Should Not Include Increased Surveillance, CTR. FOR AM. PROGRESS (Feb. 20, 2019), https://www.americanprogress.org/article/efforts-address-gun-violence-not-include-increased-surveillance/
13 Emma E. McGinty, Alene Kennedy-Hendricks, Seema Choksy & Colleen L. Barry, Trends in News Media Coverage of Mental Illness in the United States: 1995–2014, 35 HEALTH AFFS. 1121, 1124–25 (2016) reported that in the period from 1995-2014, of all news stories on mental disorders, 55% mentioned violence, and 38% mentioned interpersonal violence. About half (47%) contained a depiction of an individual with a mental disorder, most often a depiction of interpersonal violence by a person with a mental disorder (28%) and rarely a depiction of discrimination experienced by a person with a mental disorder (6%).
14 Bernice A. Pescosolido, Bianca Manago & John Monahan, Evolving Public Views on the Likelihood of Violence from People with Mental Illness: Stigma and Its Consequences, 38 HEALTH AFFS. 1735, 1735, 1741 (2019) ("[i]t appears that scientific evidence cannot correct the rhetoric surrounding mass shootings that links violence and mental illness")
15 Henry J. Steadman, Edward P. Mulvey, John Monahan, Pamela Clark Robbins, Paul S. Appelbaum, Thomas Grisso, Loren H. Roth & Eric Silver, Violence by People Discharged from Acute Psychiatric Inpatient Facilities and by Others in the Same Neighborhoods, 55 ARCH. GEN. PSYCHIATRY 393, 400, 401 (1998) describes the MacArthur Violence Risk Assessment Study, which compared the prevalence for violence among individuals with mental illnesses to the prevalence for violence among other residents of the same neighborhoods. The study showed that the two groups’ prevalence for violence was “statistically indistinguishable.” See Eric B. Elbogen & Sally C. Johnson, The Intricate Link Between Violence and Mental Disorder: Results from the National Epidemiologic Survey on Alcohol and Related Conditions, 66 ARCH. GEN. PSYCHIATRY 152, 152, 155 (2009) (“severe mental illness alone did not predict future violence; it was associated instead with historical (past violence, juvenile detention, physical abuse, parental arrest record), clinical (substance abuse, perceived threats), dispositional (age, sex, income), and contextual (recent divorce, unemployment, victimization) factors")
disorder make up over 12% of the U.S. population.\textsuperscript{16} Yet they are included as only 0.2% (1/435) of U.S. Representatives and 0% (0/7,386) of state legislators.\textsuperscript{17} In 2020, they were included as only 0.04% (3/7,636) of senior employees in cabinet-level federal departments: 0% (0/502) of senior employees at the U.S. Department of Health and Human Services (HHS), 0% of senior employees at the Substance Abuse and Mental Health Services Administration (SAMHSA), 0% (0/50) of senior employees at the National Institutes of Health (NIH) and the National Institute of Mental Health (NIMH), 0% (0/33) of senior employees at the Centers for Disease Control and Prevention (CDC), 0% (0/79) of senior employees at the Centers for Medicare and Medicaid (CMS), and 0% (0/23) of senior employees at the Health Resources and Services Administration (HRSA).\textsuperscript{18} They were included as only 2.65% of SAMHSA’s entire permanent workforce in 2016\textsuperscript{19} and less than 0.4% of U.S. physicians in 2019.\textsuperscript{20} In 2020, they were also included as 0% (0/82) of senior employees at the U.S. Department of Education, 0% (0/9) of senior employees at the Commission on Civil Rights, and 0% (0/31) of senior employees at the Commission on Civil Rights, and 0% (0/31) of senior employees at the U.S. Equal


\textsuperscript{17} Nat’l Council on Independent Living, Current Elected Officials with Disabilities, https://docs.google.com/spreadsheets/d/1cJRTo0aYkEwEa0neM4fysnMDBV45NIx9P0VG8cyKAw/edit?usp=sharing (last visited Mar. 11, 2023)


\textsuperscript{20} Zakia Nouri, Michael J. Dill, Sarah S. Conrad, Christopher J. Moreland & Lisa M. Meeks, \textit{Estimated Prevalence of US Physicians with Disabilities}, 4 JAMA NETWORK Open e211254 (revealing disability prevalence among physicians to be 3.1% overall; 0.4% for deaf or serious difficult hearing; 0.2% for blind or serious difficulty seeing; 0.9% for significant mobility impairment; <0.4% for significant psychiatric disorder; 0.3% ADHD, 0.08% for learning disability); see also Lisa M. Meeks, Ben Case, Heidi Joshi, Lisa Graves & Diane M. Harper, \textit{Prevalence, Plans, and Perceptions: Disability in Family Medicine Residencies}, 53 FAMILY MED. 338, 341 (2021) (only 7% of family medicine department chairs said they had active plans to recruit residents with disabilities; of 66 respondents, “33 (50%) reported that they have had no [residents with disabilities, or] RWD enter their program in the past 5 years, while 28 (42.4%) reported matriculating between one and two RWD. Five programs (7.6%) reported matriculating between three and five residents in the last 5 years, while no programs (0%) reported more than five RWD. Of the 68 chairs who reported data on faculty members with disabilities (FWD), over half, 47 (69.1%) stated they do not have FWD. Seventeen chairs (25%) reported one FWD and four (5.9%) reported more than one FWD.”)
C. THE SURVEILLANCE OF PEOPLE WITH MENTAL HEALTH CONDITIONS AND DISABILITIES IS A CAUSE OF THEIR EXCLUSION FROM THE WORKFORCE

I believe these numbers result from administrations and Members of Congress that seem to “care” quite a lot about our “mental health,” but not about people with mental health conditions. They “care” very much about optimizing our “mental health” and preventing it from allegedly posing safety threats, but do not care at all about including people with mental health conditions and disabilities. Administrations and Members of Congress seem to dismiss these zero inclusion numbers as indicative of problems of individuals with mental health conditions and disabilities who just need to get over themselves and their own internalized “self-stigma” and come out. Their interpretation is that individuals with mental health conditions are geographically present in the workforce, it is “just” that these workplaces are so hostile and

21 Mariel Padilla, Biden Promised the Most Diverse Administration Ever. Here’s How He’s Doing, THE 19TH NEWS (Apr. 30, 2021 11:23 AM ET), https://19thnews.org/2021/04/biden-promised-the-most-diverse-administration-ever-heres-how-hes-doing/ (emphasis added) (“Hanis said the biggest diversity gap he has seen is the representation of people with disabilities. About 1 in 4 Americans live with a disability, he said, and yet only 3 percent of all [Biden political] appointees identify as disabled. When it comes to leadership, the disparity is wider. Hanis said he is not aware of any senior officials that have disabilities.”)

prejudicial towards them, so stigmatizing, and so likely to result in discrimination for those out as having mental health conditions in the workplace, that they do not come out. That is all. Nothing to see here. No problem.

I respectfully disagree with this perspective and view this exclusion of individuals with mental health conditions in the federal workforce as a major cause of deeply problematic public policy, including public policy encouraging surveillance of individuals with mental health conditions. I also view these surveillance activities as a major reason why individuals with mental health conditions and disabilities will not come out, and as a major cause of their exclusion from the workplace.

D. IN-PERSON SURVEILLANCE OF WORKERS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES IS AT LEAST AS PROBLEMATIC AS ELECTRONIC SURVEILLANCE, LEADS TO ELECTRONIC SURVEILLANCE, AND ENHANCES ITS DISCRIMINATORY EFFECTS

My concerns here pertain to mental health surveillance and monitoring of workers in general and are not specific to electronic surveillance and monitoring. They generally concern prohibited medical (disability-related) inquiries and examinations of employees, which are themselves forms of disability discrimination under the Americans with Disabilities Act (ADA). The mental health surveillance and monitoring of workers I describe in this letter may alternatively represent other forms of disability discrimination prohibited under the ADA. Even if they are not prohibited under the ADA, however, they represent bad public policy, and the Biden administration and Congress should be discouraging rather than encouraging them.

While the OSTP’s request for information appears most interested in electronic surveillance and monitoring of workers, I argue that the in-person surveillance of workers with actual or perceived mental health conditions described in this letter will inevitably lead to electronic surveillance. Biden administration and Congressional support for legislation authorizing billions of dollars to collect data, conduct research, and implement programs effecting surveillance of individuals with actual or perceived mental health conditions and disabilities in the workplace (e.g., “encouraging [employees] to seek support and treatment for their own mental health and substance use concerns; and help[ing] such [employees] to identify

---

23 42 U.S.C. § 12112(d)(1) (“The prohibition against discrimination as referred to in subsection (a) shall include medical examinations and inquiries.”)
24 42 U.S.C. § 12112(b) (“the term ‘discriminate against a qualified individual on the basis of disability’ includes-(1) limiting, segregating, or classifying a job applicant or employee in a way that adversely affects the opportunities or status of such applicant or employee because of the disability of such applicant or employee; (2) participating in a contractual or other arrangement or relationship that has the effect of subjecting a covered entity's qualified applicant or employee with a disability to the discrimination prohibited by this subchapter (such relationship includes a relationship with an employment or referral agency, labor union, an organization providing fringe benefits to an employee of the covered entity, or an organization providing training and apprenticeship programs); (3) utilizing standards, criteria, or methods of administration—(A) that have the effect of discrimination on the basis of disability; or (B) that perpetuate the discrimination of others who are subject to common administrative control”); 42 U.S.C. § 12182(b)(1)(D) (“An individual or entity shall not, directly or through contractual or other arrangements, utilize standards or criteria or methods of administration—(i) that have the effect of discriminating on the basis of disability; or (ii) that perpetuate the discrimination of others who are subject to common administrative control.”)
risk factors in themselves and others and respond to such risks”\textsuperscript{25} and in educational settings (e.g., the “Federal Clearinghouse on School Safety Evidence-Based Practices,”\textsuperscript{26} “school threat assessment and intervention teams”\textsuperscript{27}; programs to “improve the identification and treatment for [adult] students at risk”\textsuperscript{28}; see APPENDIX I) all but guarantees the development of more covert, automated, and electronic systems to surveil these workers in the future. Automated and electronic systems may result from data collected directly pursuant to or as an indirect result of this legislation.

Perhaps most problematically, Biden administration and Congressional support for these surveillance practices lends these activities and tools great legitimacy. It sends an unmistakable message of approval for surveilling individuals with mental health conditions in the workplace. It tells employers, the public, and individuals with mental health conditions and disabilities, that they are dangerous, deficient, and dependent on mental health treatment that they are not receiving as a result of denial and poor insight. It tells them they need to be watched by their employers and their peer coworkers both for their own good and everyone else’s. Biden administration and Congressional support for these mental health awareness activities greatly enhances the discriminatory punch of other surveillance activities, including the electronic, automated worker surveillance and monitoring systems that appear to be at the heart of the OSTP’s request for information. It also detracts mightily from meaningful efforts to actually facilitate their inclusion.

In the words of Franklin Owusu-Ansah (of Owusu-Ansah v. Coca-Cola Co.), “someone [is] ‘going to pay for this.’”\textsuperscript{29} By “someone,” I mean elected and appointed officials, and by “pay,” I mean pay a political price for encouraging the stalking and surveillance of workers with actual or perceived mental health conditions and disabilities.

\textsuperscript{29} Owusu-Ansah v. Coca-Cola Co., 715 F.3d 1306, 1309 (11th Cir. 2013) (a medical inquiries/examination case described \textit{infra}).
I. A DESCRIPTION OF SURVEILLANCE AND MANAGEMENT OF STUDENTS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

A. PROMOTED IN FEDERAL GRANT PROGRAMS

The Bipartisan Safer Communities Act authorized for each of fiscal years 2022 through 2025, $240,000,000 for Project AWARE (Advancing Wellness and Resilience in Education)\(^\text{30}\) and $120,000,000 for Mental Health Awareness Training.\(^\text{31}\) The Congressional Research Service’s 2022 report on *Federal Support for School Safety and Security* summarizes that Project AWARE originated as part of the Obama Administration’s 2013 *Now Is the Time* initiative. Launched in the wake of the mass shooting at Sandy Hook Elementary School in Newtown, CT, in 2012, this plan introduced a number of activities aimed at protecting children and communities by reducing gun violence … [such as] provid[ing] training for school personnel and other adults to detect mental health issues … [and] training to school personnel and individuals working with youth on how to recognize a mental illness.\(^\text{32}\)

Many other federal programs serve similar functions, are often based in unfounded assumptions that individuals with mental health conditions are violent, and are described in the Congressional Research Service report.\(^\text{33}\)

B. PROMOTED IN FEDERAL STATUTES

The most visible efforts on the part of federal legislators to expand surveillance of people with mental health disabilities have centered on schools. These include the Bipartisan Safer Communities Act’s massive funding for “discriminatory threat assessments, which harm Black and Brown students and students with disabilities,”\(^\text{34}\) for State “crisis intervention programs,”\(^\text{35}\)

\(^{30}\) Bipartisan Safer Communities Act, Pub. L. No. 117-159, 136 Stat. 1313, 1340 (2022) (“for each of fiscal years 2022 through 2025 … $240,000,000 shall be for activities and services under Project AWARE”)

\(^{31}\) Id. (“for each of fiscal years 2022 through 2025 … $120,000,000 shall be for Mental Health Awareness Training”)


\(^{33}\) See, e.g., id. at 8 (Matching Grant Program for School Security); 17 (SchoolSafety.gov); 24 (The Edward Byrne Memorial Justice Assistance Grant (JAG) Program); 26 (Community Oriented Policing Services (COPS) Hiring Program); 31 (Garrett Lee Smith (GLS) Youth Suicide Prevention Campus Grants), among many others.

\(^{34}\) Bazelon Ctr. for Mental Health Law, Bipartisan Safer Communities Act: Advocacy Toolkit 2 (Oct. 4, 2022), https://secureservercdn.net/198.71.233.69/d25.2ac.myftpupload.com/wp-content/uploads/2022/10/Bipartisan-Safer-Communities-Act-Advocacy-Toolkit.pdf (“The Act directs the Department of Homeland Security (DHS) to establish a clearinghouse of evidence-based practices and recommendations to improve school safety. This opens the door to federal support for threat assessment programs and other school ‘hardening’ measures which would criminalize the behavior of children with disabilities, including Black and Brown students”; “school-based policing and threat assessments … have not been found to reduce gun violence in schools, and have been shown to increase use of school discipline and force, especially directed at students with disabilities and Black and Brown students.”)

\(^{35}\) Id. (“The Act creates a new fund, to be administered by DOJ over the next five years, for states to implement ‘crisis intervention programs.’ These include specialty courts such as mental health courts, which may subject participants to court supervision, and punishment, for lengthy time periods. One Senator stated that the money could
and extreme risk protection orders “or ‘red flag laws’ that violate civil rights by targeting people based purely on whether they have a mental health disability or diagnosis, rather than properly focusing on conduct or behavior.”

(See APPENDIX I for sections of the U.S.C. authorizing or contributing to mental or behavioral health surveillance in schools.)

II. A DESCRIPTION OF SURVEILLANCE AND MANAGEMENT OF WORKERS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

A. PROMOTED BY THE U.S. HHS AND ODEP

Though surveillance and management of workers with mental health conditions and disabilities has been less explicitly reinforced and encouraged in federal statute, it was encouraged by the U.S. HHS and Surgeon General’s 2012 National Strategy for Suicide Prevention, which advised that “[b]usinesses and [e]mployers [c]an [t]rain employees and supervisors to recognize coworkers in distress and respond appropriately.” The CDC’s 2018 advisory on mental health in the workplace recommends “[p]rovid[ing] managers with training to help them recognize the signs and symptoms of stress and depression in team members and encourage them to seek help from qualified mental health professionals.” The Surgeon General’s 2021 advisory similarly advises to “[p]rovide managers and supervisors with training to help recognize negative mental health symptoms in themselves and colleagues and encourage employees to seek help from qualified mental health professionals.” The Surgeon General’s 2022 Framework for Workplace Mental Health & Well-Being provides as an example to emulate, a university that developed “workshops to help supervisors identify and respond appropriately,” which advised that “provide[ing] managers with training to recognize coworkers in distress and respond appropriately.” In August 2022, SAMHSA released an advisory on “Expanding Implementation of Mental Health Awareness Training in the Workplace.”

also fund involuntary commitment programs, coerced mental health treatment that has not been shown to outperform voluntary services and which may disproportionately impact Black and Brown people.”

36 Id. at 3; compare U.S. Dep’t of Justice, Commentary for Extreme Risk Protection Order Model Legislation (June 7, 2021), https://www.justice.gov/d9/pages/attachments/2021/06/07/erpo-model-legislation_0.pdf (“Research has shown that states can save lives by authorizing courts to issue extreme risk protection orders (ERPOs) that temporarily prevent a person in crisis from accessing firearms”) with Sierra Smucker, Effects of Extreme Risk Protection Orders on Suicide, RAND CORP. (Jan. 10, 2023), https://www.rand.org/research/gun-policy/analysis/extreme-risk-protection-orders/suicide.html (“Evidence for the effect of extreme risk protection orders on total and firearm suicides is inconclusive”); see also Extreme Risk Protection Order Expansion Act 2023, S. 247, 118th Cong. (1st Sess. 2023)


The U.S. Department of Labor’s Office of Disability Employment Policy (ODEP) has been no better. As ODEP explained in 2020:

Mental health in the workplace has received heightened national attention and is a major interest of stakeholders, including its potential relationship to workplace violence and individual experiences during the COVID-19 pandemic. To address this demand, ODEP’s employer technical assistance center, the Employer Assistance and Resource Network on Disability Inclusion (EARN), created the award-winning Mental Health Toolkit).

I met with ODEP leaders together with several colleagues with lived experience of workplace disability discrimination through mental health surveillance, to express our serious concerns with the content of this toolkit and its recommendations to “empower your managers and supervisors to recognize warning signs,” “educate managers on recognizing signs of stress in employees,” and “[p]rovid[e] screening for mental health conditions and substance use disorders.”

We were also concerned with the content of the resources it promoted for employers, which were authored by organizations heavily funded by pharmaceutical companies, like the American Psychiatric Association Foundation and the National Alliance on Mental Illness (NAMI), an organization representing the interests of parents and family members of individuals with mental health conditions. These resources, for example, advise to “[t]rain leaders to

45 Employer Assistance & Res. Network on Disability Inclusion (EARN), Pillar 3: Offer Employee ASSISTANCE, https://askearn.org/page/pillar-3-offer-employee-assistance (last visited May 4, 2023) (recommending “[p]roviding screening for mental health conditions and substance use disorders”); see also Employer Assistance & Res. Network on Disability Inclusion (EARN), Model Successful Programs, https://askearn.org/page/model-successful-programs (last visited May 4, 2023) (“DuPont’s global EAP team created and implemented an internal anti-stigma campaign, called ‘ICU’ (‘I See You’), the centerpiece of which is an animated video about how to recognize signs of emotional distress in colleagues and encourage them to seek help.”)
47 Nat’l All. on Mental Illness (NAMI) Wisconsin, Mission, https://web.archive.org/web/20140602200704/http://www.namiwisconsin.org/mission.cfm (last visited Dec. 26, 2022) (“NAMI was formed in 1977 [in Madison, WI] when Harriet Shetler and Beverly Young, two mothers, each with a son with schizophrenia, met over lunch to discuss the similar challenges they shared raising a child with a serious mental illness.”); Emily Shrader, The History of NAMI National, NAMI Pennsylvania, and NAMI PA Cumberland and Perry Counties (Dec. 2011), https://web.archive.loc.gov/all/20140514000152/http://www.nami.org/Content/Microsites316/NAMI_PA_Cumberland_and_Perry_Cos/Home310/About_Us_Board_of_Directors/The_History_NAMI.pdf (“These women were upset with the lack of services for their sons and the mothers were tired of being blamed for the sons’ mental illnesses.”);
identify emotional distress and refer to [employee assistance program] EAP or other behavioral health resources,”48 “give employees and managers the knowledge and tools to recognize depression and intervene at an early stage to help affected colleagues,”49 and “[p]rovide training in identifying job performance problems related to mental health issues,”50 and “[p]rovide Health Risk Appraisals (HRA) to employees that include mental health questions and questions about management and supervisor support for team member health. Include questions related to stress, depression, and substance use disorders in health risk appraisals.”51 They state that “[e]mployers can play a key role in supporting the early identification of depression and other mental health conditions.”52

ODEP also directs employers to resources from Right Direction, “an initiative from the American Psychiatric Association Foundation’s Center for Workplace Mental Health and Employers Health, a professional benefits organization. Right Direction is supported by Takeda Pharmaceuticals U.S.A., Inc. (TPUSA) and Lundbeck U.S.” pharmaceuticals.”53 Its manager training webinar54 tells managers to “[r]ecognize the [s]igns of depression, and cites several DSM-5 diagnostic criteria (e.g., “Feelings of sadness,” and “Sleep disturbance”), and also makes unfounded55 claims that “[s]igns of depression include “[p]oor quality work,” “[p]rocrastination, accidents on the job,” “[i]ndecisiveness, slowed productivity,” “[p]resenteeism—’just showing up,’” “[m]issed deadlines, absenteeism,” “[p]oor relationships with co-workers, a boss, clients,” “[l]ow morale,” and “[l]ate to work.”

---

48 Nat’l All. on Mental Illness (NAMI), Major Corporate and Foundation Contribution Registry: 2nd Quarter 2022 (last visited Dec. 27, 2022), https://www.nami.org/NAMI/media/NAMI-Media/PDFs/Financials/Q2-2022-Web-Registry_Final.pdf (includes Alkermes [biopharmaceutical company] ($200,000); Axsome Therapeutics [biopharmaceutical company] ($35,000); Stanley Center for Psychiatric Research Broad Institute of MIT and Harvard ($30,000); Cerevel Therapeutics [biopharmaceutical company] ($15,000); Google LLC ($5,000); Neurorine Biosciences, Inc. [biopharmaceutical company] ($370,000); Novo Nordisk, Inc. [biopharmaceutical company] ($75,000); Otsuka America Pharmaceutical, Inc. [biopharmaceutical company] ($69,087); Takeda Pharmaceuticals America, Inc. [biopharmaceutical company] ($100,000); Teva Pharmaceuticals [biopharmaceutical company] ($25,000)).
49 Id. at 17.
50 Id. at 22.
51 Id. at 23 (“Provide information and EAP to those who screen positive. Consider having EAP reach out to positive screens rather than relying on the individual to follow up”)
53 See Nicholas D. Lawson, “To Be a Good Lawyer, One Has to Be a Healthy Lawyer”: Lawyer Well-Being, Discrimination, and Discretionary Systems of Discipline. 34 GEO. J. LEGAL ETHICS 65, 85-88 (2021) (“Claims That Workers with Mental Health Disorders Are Less Productive and Are Economically Burdensome to Their Employers Are Flawed”)
My colleagues and I did feel that ODEP leaders took our concerns seriously. Rather than value the perspectives of individuals with mental health conditions and lived experience of mental disability discrimination in the workplace, ODEP instead, continues to elevate, promote, and disseminate materials produced by professional, parent, and pharmaceutical-funded organizations (e.g., the American Psychiatric Association Foundation, NAMI) and EAP businesses. EAP services include workplace violence consultations (80%), referrals of employees to HR/management (68%), consultations with HR/manager on employee performance issues (63%), and evaluations of employees for fitness for duty. With respect to EAP effectiveness, studies “have fallen short in demonstrating the actual effect of obtaining a positive effect in the workplace.” Even the National Institute on Alcohol Abuse and Alcoholism has acknowledged that “despite the widespread use of [EAPs], no data from a representative sample of EAPs are available to support the usefulness of these programs” and “[n]one of the studies involved rigorous comparisons with settings where no EAP services are available.”

The materials disseminated by HHS, the Surgeon General, and ODEP are highly stigmatizing and misleading. They send an unmistakable message that workers with actual or suspected mental health conditions are dangerous, deficient, dependent on mental health treatment that are not receiving as a result of denial and poor insight, and need to be watched and referred by their employers and peer coworkers. Such guidance and materials all-but guarantee that individuals with mental health conditions and disabilities will remain excluded from the workforce and experience discrimination.

**B. PROMOTED IN RECENT AND PROPOSED FEDERAL LEGISLATION SINCE 2021**

Not counting the “drug-free workplace legislation [that] was passed in 1988 [(which] spurred further growth of EAPs”), the American Rescue Plan Act of 2021 and Dr. Lorna Breen Health Care Provider Protection Act of 2022 are, to my knowledge, the first modern federal statutes to actively encourage ongoing surveillance and monitoring of workers with mental health conditions and disabilities by their employers and coworkers.

---

56 See Nicholas D. Lawson, supra note 43.

57 See, e.g., EMPLOYEE ASSISTANCE & RES. NETWORK ON DISABILITY INCLUSION (EARN), Pillar 3: Offer Employee ASSISTANCE, [https://askearn.org/page/pillar-3-offer-employee-assistance](https://askearn.org/page/pillar-3-offer-employee-assistance) (last visited May 23, 2023) (enthusiastically trumpeting EAPs and including various misleading claims, including that “[r]esearch conducted over the years has affirmed EAPs’ effectiveness, for both employers and employees, on multiple levels.”)


59 David Weiss, Employee Assistance Programs and Behavioral Health Disability, in HANDBOOK OF BEHAVIORAL HEALTH DISABILITY MANAGEMENT 289, 311 (Pamela A. Warren ed., 2018) (observing that case studies or testimonials have “limited value to document the effectiveness of EAP services,” that utilization rates “only indicate[] the extent to which employees use the EAP [and] do not provide any objective data regarding whether the EAP had a positive workplace impact”)


Section 2703 of the American Rescue Plan Act of 2021 appropriated to the HHS Secretary $80,000,000 for FY 2021 to award to “health professions schools, academic health centers, State or local governments, Indian Tribes and Tribal organizations, or other appropriate public or private nonprofit entities” “to plan, develop, operate, or participate in health professions and nursing training activities for health care students, residents, professionals, paraprofessionals, trainees, and public safety officers, and employers of such individuals, in evidence-informed strategies for reducing and addressing suicide, burnout, mental health conditions, and substance use disorders among health care professionals.”

Section 2704 appropriated $20,000,000 for FY 2021 for the HHS Secretary and CDC Director, “in consultation with the medical professional community” “to carry out a national evidence based education and awareness campaign directed at health care professionals and first responders (such as emergency medical service providers), and employers of such professionals and first responders. Such awareness campaign shall— (1) encourage primary prevention of mental health conditions and substance use disorders and secondary and tertiary prevention by encouraging health care professionals to seek support and treatment for their own mental health and substance use concerns; and (2) help such professionals to identify risk factors in themselves and others and respond to such risks.”

Lastly, Section 2705 appropriated $40,000,000 for the HHS Secretary and HRSA Administrator “to award grants or contracts to entities providing health care, including health care providers associations and Federally qualified health centers, to establish, enhance, or expand evidence-informed programs or protocols to promote mental health among their providers, other personnel, and members.”

The Dr. Lorna Breen Health Care Provider Protection Act of 2022 extended the funding appropriated for purposes identified in §§ 2703-2705 of the American Rescue Plan Act of 2021 with minor modifications. Not surprisingly, the situation today is that “some residency programs require all trainees be evaluated by psychology and psychiatry services.”

The proposed Supporting the Mental Health of Educators and Staff Act of 2023 (“To address behavioral health and well-being among education professionals and other school staff”) is modeled closely on the Dr. Lorna Breen Health Care Provider Protection Act (“To address behavioral health and well-being among health care professionals”) and adopts identical language (“to encourage [education and] health care professionals to seek support and care for

---

63 § 2704, 135 Stat. at 46.
64 § 2705, 135 Stat. at 46-47.
65 Dr. Lorna Breen Health Care Provider Protection Act, Pub. L. No. 117–105, § 3-4, 136 Stat. 1118, 1118-19 (2022) (codified at 42 U.S.C. § 294t) (“improving awareness among health care professionals about risk factors for, and signs of, suicide and mental health or substance use disorders”; “encourage health care professionals to seek support and care for their mental health or substance use concerns, to help such professionals identify risk factors associated with suicide and mental health conditions, and to help such professionals learn how best to respond to such risks”)
66 Richard Balon & Mary Morreale, The Madness of Mandated Wellness, 31 ANNALS OF CLINICAL PSYCHIATRY 81, 82 (2019) (emphasis added) (“In order to demonstrate concern and provide evidence of intervention, some residency programs require all trainees be evaluated by psychology and psychiatry services.”)
their mental health or substance use concerns, to help such professionals identify risk factors associated with suicide and mental health conditions, and to help such professionals learn how best to respond to such risks.” 67). Their goals are described as reducing the “prevalence and severity of mental health conditions and substance use disorders among education professionals and other school staff” 68 and reducing the “prevalence and severity of mental health conditions and substance use disorders among health professionals.” 69

The proposed Providing Resources and Occupational Training for Emotional Crisis and Trauma (PROTECT) in 911 Act (“To require the Secretary of Health and Human Services to improve the detection, prevention, and treatment of mental health issues among public safety telecommunicators”) requires the Secretary of HHS to “develop and make publicly available evidence-based best practices to identify, prevent, and treat posttraumatic stress disorder and co-occurring disorders in public safety telecommunicators.” 70

The proposed DHS Suicide Prevention and Resiliency for Law Enforcement Act requires the Secretary of HHS to “conduct data collection and research on mental health, suicides, and, to the extent possible, attempted suicides, of law enforcement personnel within the Department of Homeland Security” and to “promote education and training related to mental health, resilience, suicide prevention, stigma, and mental health resources to raise mental health awareness and to support others the needs of supervisors, clinicians, care-givers, peer support members, chaplains, and those who have been exposed to trauma.” 71

C. WHY THESE AWARENESS ACTIVITIES UNDERMINE THE SPIRIT IF NOT THE LETTER OF THE LAWS PROHIBITING MEDICAL (DISABILITY-RELATED) INQUIRIES OF CURRENT EMPLOYEES UNDER THE ADA

To appreciate the harms associated with these workplace mental health awareness activities, it is worth reviewing the intended purpose and functions of ADA prohibitions on medical inquiries.

67 Compare Supporting the Mental Health of Educators and Staff Act of 2023, H.R. 744, 118th Cong. § 3 (1st Sess. 2023) (“in consultation with relevant stakeholders, including medical professional associations, shall establish a national evidence-based or evidence-informed education and awareness initiative—(1) to encourage education professionals and other school staff to seek support and care for their mental health or substance use concerns, to help such professionals and staff identify factors associated with risks for suicide and mental health conditions, and to help such professionals learn how best to respond to such risks”) with § 3, 136 Stat. at 1118 (“in consultation with relevant stakeholders, including medical professional associations, shall establish a national evidence-based or evidence-informed education and awareness initiative— (1) to encourage health care professionals to seek support and care for their mental health or substance use concerns, to help such professionals identify risk factors associated with suicide and mental health conditions, and to help such professionals learn how best to respond to such risks”)

68 H.R. 744, § 6; see also id. at § 5 (“assessing the prevalence and severity of mental health conditions among education professionals and other school staff”)

69 § 6, 136 Stat. at 1120.

70 Providing Resources and Occupational Training for Emotional Crisis and Trauma (PROTECT) in 911 Act, H.R. 2763, 118th Cong. § 2 (1st Sess. 2023)

71 DHS Suicide Prevention and Resiliency for Law Enforcement Act, S. 1137, 118th Cong. § 2 (1st Sess. 2023); DHS Suicide Prevention and Resiliency for Law Enforcement Act, H.R. 2577, 118th Cong. § 2 (1st Sess. 2023) (also requiring the Secretary to “promote a culture that reduces the stigma of seeking mental health assistance through regular messaging, training, and raising mental health awareness”)

1353
1. The Purpose of the ADA’s Prohibitions on Disability-Related Inquiries of Current Employees

The medical (disability-related) inquiries provision of the ADA was designed to protect employees with “‘hidden’ disabilities such as epilepsy, diabetes, emotional illness, heart disease and cancer” from exclusion resulting from acquisition of private medical information that could reveal their disability status, as Congress recognized that “[b]eing identified as having a disability often carries both blatant and subtle stigma.” It recognized that unwarranted disability-related inquiries and medical examinations “serve[] no legitimate employer purpose, but simply serve[] to stigmatize the person with a disability.”

(a) Why Privacy Protections for Current Employees with Mental Health Conditions Are Particularly Important

Among employees with “hidden” disabilities, those with “emotional” (mental) illnesses may particularly benefit from privacy protections because mental disorders in general are more highly stigmatized by employers. Employees both with serious mental illness and those with relatively mild, common mental health conditions need workplace privacy protections. Fears, myths, and stereotypes that persons with mental health conditions are dangerous and incompetent are not limited to severe mental illnesses (e.g., schizophrenia, bipolar disorder); some even argue that “the label of mental disorder exerts its strongest effects when it accompanies normal-range behavior patterns or mild disturbance,” such as anxiety or

74 Id.
75 See, e.g., Mara Pheister, Rachel M. Peters & Marika I. Wrzosek, The Impact of Mental Illness Disclosure in Applying for Residency, 44 ACAD. PSYCHIATRY 554, 554 (2020) (“Applicants who disclosed a history of depression had higher odds of being in a lower category of receiving an invitation (OR = 3.60, p < .001 for a ‘perfect’ applicant, OR = 2.39, p < .001 for a ‘good’ applicant with leave of absence) and a lower category for match ranking (OR = 1.94, p = .01 for a perfect applicant, OR = 2.30, p < .001 for a good applicant with leave of absence) compared with the candidate who disclosed a history of diabetes.”)
Crosby Hipes, Jeffrey Lucas, Jo C. Phelan & Richard C. White, The Stigma of Mental Illness in the Labor Market, 56 SOC. SCI. RES. 16, 20 (2016) (“14.81% of our fictitious candidates with a history of mental illness received callbacks, compared to 21.86% of candidates with a history of physical injury.”);
Lily R. Ren, Ramona L. Paetzold & Adrienne Colella, A Meta-Analysis of Experimental Studies on the Effects of Disability on Human Resource Judgments, 18 HUM. RESOURCE MGMT. REV. 191, 200 (2008) (summarizing that the results reflected that “mental disabilities were shown to have a more negative effect on performance expectations and hiring decisions than physical disabilities. These findings are consistent with a vast literature on stigmatization of persons with mental disabilities, causing them to be seen less as ideal employees and more as potentially difficult, even dangerous, individuals, despite evidence to the contrary. Most of the works included in our meta-analysis involving mental disabilities Most of the works included in our meta-analysis involving mental disabilities examined depression [5/9]. However, we would anticipate even more negative findings for mental illnesses such as bipolar disorder or schizophrenia, which are often viewed as more incapacitating and dangerous by laypersons”) (citations omitted)

Denise A. Koser, Munehiko Matsuyma & Richard E. Kopelman, Comparison of a Physical and a Mental Disability in Employee Selection: An Experimental Examination of Direct and Moderated Effects, 1 N. AM. J. PSYCHOL. 213, 217 (1999) (finding that an applicant who uses a wheelchair was 7-times more likely to be hired than an employee taking medication for depression or anxiety.)
76 See Stephen P. Hinshaw & Andrea Stier, Stigma as Related to Mental Disorders, 4 ANN. REV. CLINICAL PSYCHOL. 367, 375-6 (2008) (“current psychiatric nomenclatures now incorporate a huge number of syndromes and problems that used to fall within the bounds of normal human variation. Because the terms ‘mental disorder’ or ‘mental
depressive disorders, specific learning disorders, and other common mental health conditions. Indeed, some argue that “employer scrutiny of those with hidden behavioral anomalies is likely to be worse than employer scrutiny of persons with more obvious mental disorders or with physical disabilities,” 77 as “‘hidden’ impairments may be particularly mysterious and thus particularly subject to fear and stereotypes.” 78 Altogether, it may be especially important for these employees to keep their disabilities hidden through privacy protections in the workplace.

Privacy protections may be important for employees with common mental health conditions that are non-obvious and who may never need to request workplace accommodations. They may never need accommodations necessitating disclosures to their employer that may ultimately “out” their private mental health information. Accordingly, they may have every reason to wish to maintain their mental health information from their employers. 79

There are many reasons why privacy may be especially important for employees with mental health conditions to advance autonomy, or the freedom and capacity to make life decisions, with regard to mental health treatment. Optimal treatments for many physical health conditions, for instance, are often supported by a strong body of evidence. There is broad consensus in general medicine, for example, about the benefits of daily aspirin as prophylaxis for adverse coronary events in patients with heart disease. But in psychiatry, there is often very little consensus about the appropriateness of suicide prevention strategies, or on which treatments, interventions, or behaviors, are appropriate for which individuals with mental health conditions. 80 Employers may have strong personal opinions about particular mental health therapies and remedies, and employees with mental health conditions may want to avoid any disclosures inadvertently inviting these employers to impose personal treatment preferences on their employees.

Lastly, employers, professionals, judges, 81 and experts, are highly susceptible to widely-held myths, fears, and stereotypes of dangerousness and incompetence of persons with mental illness’ now encompass a wide variety of behaviors and emotional styles, more forms of deviance are likely to receive stigma, related to the invocation of the mental illness label.” (citation omitted)

77 See John M. Casey, From Agoraphobia to Xenophobia: Phobias and Other Anxiety Disorders Under the Americans with Disabilities Act, 17 U. Puget Sound L. Rev. 381, 416 (1994)


79 See Purvi Sevak & Shamima Khan, Psychiatric Versus Physical Disabilities: A Comparison of Barriers and Facilitators to Employment, 40 Psychiatric Rehabilitation J. 163 (2017) (findings suggesting that nonemployment among persons with mental health disabilities (compared with physical disabilities) are less often related caused by medical impairments and more often related to social discrimination.)

80 See Jennifer Radden, Public Mental Health and Prevention, 11 Pub. Health Ethics 126, 126 (2018) (“To suppose that public mental health can be entirely modeled on other public health programs is mistaken. Instead, it must proceed with awareness of the particular features typifying many mental disorders. These include (i) features of the disorders themselves; (ii) the preliminary nature of scientific knowledge about them; (iii) the contested applicability of traditional disease models to them; (iv) the dearth of established research data available about preventive interventions currently in place or proposed; and (v) the effects of stigma and discrimination on any such interventions.”).

81 See, e.g., Michael L. Perlin & Heather Ellis Cucolo, Pretextuality, in Mental Disability Law: Civil and Criminal § 2-3 (3d ed. 2016) (“courts regularly accept (either implicitly or explicitly) testimonial dishonesty, countenance liberty deprivations in disingenuous ways that bear little or no relationship to case law or to statutes and engage similarly in dishonest (and frequently meretricious), decisionmaking, specifically where witnesses,
disabilities\textsuperscript{82} that continue to make recourse to discrimination for these employees exceedingly rare.

(b) Privacy Protections Preempt Employment Discrimination Before It Occurs and Offer Other Antidiscrimination Advantages

Given that litigants challenging employment discrimination on the basis of mental disability have traditionally fared quite poorly, interventions to combat employment discrimination after it occurs may be too late. An important advantage of privacy law in reducing discrimination is that it is preemptive and may render subsequent discrimination impossible by restricting access to the information discriminators need to discriminate. Privacy law also poses fewer burdens of proof to those who report discrimination. Whereas traditional antidiscrimination law often requires proof of discriminatory intent, privacy law requires only proof of unwarranted employer access to protected information. “It is a straightforward factual inquiry instead of an attempt to divine a potential discriminator’s true intent, to the exclusion of all other possible explanations.”

Privacy approaches also have the advantage of removing the focus of inquiry away from employees’ stigmatized disability status. Prior to passage of the ADA Amendments Act in 2008, judicial analysis of ADA employment discrimination claims “focus[ed] on the threshold question of whether someone actually has a disability—even to the exclusion of considering an employer's motives,”\textsuperscript{84} prompting Congress to expand antidiscrimination protections for those “regarded as” disabled. Perhaps not surprisingly in light of the prejudice associated with these

\begin{itemize}
  \item especially expert witnesses, show a ‘high propensity to purposely distort their testimony in order to achieve desired ends.’ […] Judges in mental disability law cases often take relevant literature out of context, misconstrue the data or evidence being offered, and/or read such data selectively, and/or inconsistently. Other times, courts choose to flatly reject this data or ignore its existence. In other circumstances, courts simply ‘rewrite’ factual records so as to avoid having to deal with social science data that is cognitively dissonant with their view of how the word ‘ought to be.’” (citations omitted)
\end{itemize}

\textsuperscript{82} See, e.g., Bernice A. Pescosolido, Tait R. Medina, Jack K. Martin & J. Scott Long, The “Backbone” of Stigma: Identifying the Global Core of Public Prejudice Associated with Mental Illness, 103 AM. J. PUBLIC HEALTH 853, 856 (2013) (study provided members of the general public vignettes of a person with depression and found many respondents believed the person “shouldn’t hold public office” (41%), “shouldn’t supervise others” (48%), “shouldn’t teach children” (55%), would be “unwilling to work closely” with the person (32%), felt the person was “not as productive” (46%), “likely to be violent to others” (35%), “likely to be violent to self” (67%), etc.; Pescosolido et al., supra note 18, at 1735, 1739, found that from 1996, to 2006, to 2018, “perceptions regarding potential violence and support for coercion generally rose,” even for common mental disorders like depression, and “daily troubles.” The authors remarked, at 1741, “It appears that scientific evidence cannot correct the public and political rhetoric surrounding mass shootings that links violence and mental illness. Emboldened by political arguments, daily reports of impersonal violence, and media mentions linking mental illness and crime, members of the public may be expected to continue to support the stigma of dangerousness and call for the return of mental asylums as suggested recently by politicians.”

\textsuperscript{83} See Jessica L. Roberts, Protecting Privacy to Prevent Discrimination, 56 WM. & MARY L. REV. 2097, 2154 (2015) (citation omitted)

\textsuperscript{84} See Bradley A. Areheart, When Disability Isn’t “Just Right”: The Entrenchment of the Medical Model of Disability and the Goldilocks Dilemma, 83 IND. L.J. 181, 182, 209 (2008) (“Restrictive interpretations of the ADA have thus engendered a situation in which many cases are decided solely by looking at the characteristics of the plaintiff. The definition of disability may thus create the absurd result of a person being disabled enough to be fired from a job, but not disabled enough to challenge the firing.”).
conditions, appraisals that focused on these employees’ impairments resulted in very poor outcomes for these employees.

Privacy’s factual inquiry into employers’ access—rather than employers’ discriminatory intent—may also strike employers and the courts as fairer, and its prohibitions on specific conduct (i.e., prohibited inquiries) may create clear, workable standards for regulatory purposes. Most members of the general public worldwide endorse some level of mental health prejudice, and many employers probably will harbor some level of discriminatory animus toward persons with mental health conditions. These biases may often be implicit and not be subject to employer control. Direct regulation of employers’ behaviors (i.e., access or attempts to access protected information) rather than beliefs, might strike some employers and the courts as more appropriately holding them responsible for what that they can control. An antidiscrimination approach that preemptively addresses written employment policies and guidance that encourage mental health surveillance may be especially effective for similar reasons.

Privacy approaches to antidiscrimination may also be received more favorably by a conservative bench. Civil rights scholars have observed the Supreme Court shifting “from emphasizing group-oriented equality-based dignity claims to emphasizing more universal liberty-based dignity claims.”

2. WHY THESE AWARENESS ACTIVITIES UNDERMINE ADA PROHIBITIONS ON DISABILITY-RELATED INQUIRIES

Bearing in mind the intended purpose of the ADA’s prohibitions on medical inquiries, it is worth considering whether the mental health awareness activities described supra conflict with this law and its intended purpose.

According to the EEOC, a medical inquiry, also known as a “‘disability-related inquiry’ is a question (or series of questions) that is likely to elicit information about a disability” made by an employer (or the employer’s agent, see infra). Disability-related inquiries may include:

• “asking an employee whether s/he has (or ever had) a disability or how s/he became disabled or inquiring about the nature or severity of an employee's disability”;
• “asking an employee's co-worker, family member, doctor, or another person about an employee's disability”;
• “asking an employee whether s/he currently is taking any prescription drugs or medications, whether s/he has taken any such drugs or medications in the past, or monitoring an employee's taking of such drugs or medications.”

---

85 Inquiries and regulations into employers’ beliefs might also strike some as inconsistent with privacy principles to prevent “giving government the power to control men’s minds.” Stanley v. Georgia, 394 U.S. 557, 560 (1969).
88 Id.
It is worth reviewing the language of the guidance and statutes mentioned previously to discern if they encourage disability-related inquiries of employees. U.S. HHS guidance advises providing “managers with training to help them recognize the signs and symptoms of stress and depression in team members,” advises ensuring that workers “learn to recognize the signs of distress, mental health challenges and burnout in yourself and in your colleagues,” and “help[ing] supervisors identify and respond to signs of depression among staff.” The ACGME asks employers at residency programs to “educate faculty members and residents in identification of the symptoms of burnout, depression, and substance use disorder” and “encourage residents and faculty members to alert the program director or other designated personnel or programs when they are concerned that another resident, fellow, or faculty member may be displaying signs of burnout, depression, a substance use disorder.” (See APPENDIX III.) ODEP resources advise that “[e]mployers can play a key role in supporting the early identification of depression and other mental health conditions,” recommend “giv[ing] employees and managers the knowledge and tools to recognize depression and intervene at an early stage to help affected colleagues,” and train managers to “[r]ecognize the [s]igns” of depression in workers. Section 2704 of the American Rescue Plan Act, referring to “mental health conditions and substance use disorders,” advises “help[ing] such professionals to identify risk factors in themselves and others and respond to such risks.”

The Dr. Lorna Breen Health Care Provider Protection Act of 2022 aims at “improving awareness among health care


professionals about risk factors for, and signs of, suicide and mental health or substance use disorders” in health care professionals.  

(a) Disability-Related?

To count as a disability-related inquiry, an inquiry must be likely to “elicit information about a disability.” Though proponents of mental health awareness activities often use language encouraging identification of mental health “concerns,” mental health “challenges,” “warning signs,” signs of “distress,” signs of “stress,” “burnout,” poor “well-being,” or their risk factors, they are also often explicit in encouraging identification of mental health conditions (e.g., depression), which are disabilities. In other words, they seek information about disabilities.

(b) Disability-Related Inquiry?

Proponents of these mental health awareness activities might argue that the above should not be construed as recommendations to engage in disability-related inquiries because they do not specifically recommend asking “a question (or series of questions) that is likely to elicit information about a disability.” Instead, as phrased, they encourage employers and coworkers to “recognize,” “identify,” or become “aware[]” of other employees’ mental health conditions, but do not explicitly encourage them to ask questions about employees’ mental health conditions: they don’t use the magic words: “ask your employees questions likely to elicit information about a disability.”

What they encourage, in essence, is for everyone in the workplace to incorporate disability-related inquiries into their everyday interpersonal interactions in the workplace. That is, when you are at the coffee machine with a colleague who says she really needs coffee, continue the conversation, but be sure to become aware of whether or not she might need coffee because she is depressed and has not been able to sleep. Keep having those conversations with your colleagues about workplace anxieties and how they spend their personal time, but also use those casual conversations as an opportunity to become aware of, to recognize, and to identify whether or not they have mental health conditions.

On closer inspection, I believe these recommended mental health awareness activities would turn out to be recommendations to engage in “a series of questions[] that is likely to elicit information about a disability.” But because they generally stop short of explicitly making such recommendations in an obvious way, they are difficult to fight.

(c) Disability-Related Inquiry by Employer?

99 But see U.S. EQUAL EMPLOYMENT OPPORTUNITY COMM’N, supra note 87 (noting that “[t]he prohibition against making disability-related inquiries applies to inquiries made directly to an employee, as well as to indirect or surreptitious inquiries such as a search through an employee's belongings to confirm an employer's suspicions about an employee's medical condition,” and citing Doe v. Kohn Nast & Graf, P.C., 866 F. Supp. 190, 3 AD Cas. (BNA) 1322 (E.D. Pa. 1994) (employer conducted an unlawful medical inquiry when it searched the office of an employee it knew was sick and discovered a letter indicating the employee had AIDS)).
The recommended mental health awareness activities described above often encourage “[e]mployers,” “program director[s],” “managers,” “supervisors,” and “faculty members” to identify workers with mental health conditions, but they also ask workers, “colleagues” to identify mental health conditions in their peer coworkers. Sometimes, they explicitly recommend these workers report other coworkers suspected of having mental health conditions to their employers (e.g., the ACGME asks “residents and faculty members to alert the program director or other designated personnel or programs when they are concerned that another resident, fellow, or faculty member may be displaying signs of burnout, depression, a substance use disorder.” In general, however, it is difficult to establish that these workers are acting on behalf of their employers when they engage in disability-related inquiries of their coworkers and report these coworkers to their employers. Accordingly, it is difficult to establish that these workers are acting as agents of their employers when they engage in these activities, and it is therefore difficult to establish that they are disability-related inquiries made by employers.

Even so, encouraging workers to engage in awareness activities if not disability-related inquiries of their coworkers is a severe violation of the spirit and intent of the ADA’s prohibition on disability-related inquiries. EEOC guidance on disability-related inquiries, for example, contain strict rules that worker “[m]edical information must be kept confidential. The ADA contains narrow exceptions for disclosing specific, limited information to supervisors and managers, first aid and safety personnel, and government officials investigating compliance with the ADA,” but no exceptions for coworkers.

III. IT IS PREMATURE TO TURN ATTENTION AWAY FROM IN-PERSON SURVEILLANCE OF WORKERS THROUGH MEDICAL (DISABILITY-RELATED) INQUIRIES AND EXAMINATIONS

In my opinion, it is hypocritical of the Biden administration to present itself as a critic of surveillance and monitoring of workers with mental health conditions and disabilities when it has already done so much to encourage their surveillance. At the very least, it is premature to turn any attention away from in-person surveillance of workers through medical inquiries and examinations, though I commend Biden administration efforts to combat automated, electronic worker surveillance and big data.

A. EXPLAINING PROGRESSIVE CONCERNS WITH ELECTRONIC SURVEILLANCE OF WORKERS, BUT NOT WITH MEDICAL (DISABILITY-RELATED) INQUIRIES/EXAMINATIONS, AND WHY THE LATER REPRESENT AN OVERLOOKED THREAT

As Professors Bradley A. Areheart and Jessica L. Roberts put it, “in the age of big data, when employers can access information through a variety of sources other than medical

101 U.S. Equal Emp’t Opportunity Comm’n, EEOC No. 915.002, Enforcement Guidance: Preemployment Disability Related Questions and Medical Examinations (1995) (“Employers may also disclose medical information to state workers' compensation offices, state second injury funds, or workers' compensation insurance carriers in accordance with state workers' compensation laws and may use the medical information for insurance purposes”; “Does the employer's confidentiality obligation extend to medical information that an individual voluntarily tells the employer? Yes.”)
examinations and inquiries, the ADA’s privacy protections look obsolete.” Yet there are good reasons other than the programs and legislation mentioned above to believe that medical examinations and inquiries will continue to pose important privacy threats to employees.

1. RISE OF EAP/WELLNESS PERSONNEL IN THE WORKPLACE

The rise of wellness programs and occupational mental health workers, including psychologists, social workers, other therapists, EAP or wellness program personnel, plainly suggests continuing in-person interactions with these personnel and privacy threats from these interactions. And many “cases that have addressed psychological or psychiatric testing of employees or job applicants as a violation of the ADA” concern EAPs. These personnel are more likely to be making medical inquiries and conducting medical exams than to be developing software to collect and deploy big data.

Medical inquiries and examinations, especially when conducted through EAPs are almost impossible to challenge in part because (1) most courts have held that referrals to EAPs or other entities that engage in medical inquiries or examinations do not constitute adverse employment actions for the purposes of establishing either a discrimination or a retaliation complaint; (2)

103 See Kenneth Matos & Ellen Galinsky, 2012 National Survey of Employers, FAMILIES & WORK INST. (2012), http://familiesandwork.org/site/research/reports/NSE_2012.pdf. (surveyed 1,126 private employers with 50 or more employees and found prevalence of Employee Assistance Programs rose from 46% (2005) to 74% (2012); prevalence of wellness programs rose from 47% (2005) to 63% (2012)).
106 For Title VII cases holding that such referrals do not constitute adverse employment actions, see Pumpidio v. Sch. Bd. of Miami-Dade Cty., FL., No. 02-22548-CIV., 2003 WL 23312750, at *7 (S.D. Fla. Nov. 6, 2003) (“Referring the Plaintiff to the Employee Assistance Program, threatening him with termination, or complaining to him about his work performance, too, do not rise to the level required for a finding of an adverse employment action” under Title VII); Delia v. Donahoe, 862 F.Supp.2d 196, 202 (E.D.N.Y.2012) (EAP referral is not an adverse action under Title VII); Choulagh v. Holder, No. 10-14279, 2012 WL 2891188, at *8 (E.D. Mich. July 16, 2012) (“recommendng that Plaintiff explore an EAP referral cannot be view as an adverse employment action” under Title VII); Ndzerre v. Washington Metro. Area Transit Auth., 275 F. Supp. 3d 159, 166 (D.D.C. 2017) (“plaintiff has not cited—and this Court has not found—a single case where a Court has held that referral to an EAP constitutes an adverse employment action. To the contrary, the weight of authority indicates that referral to an EAP does not constitute an adverse employment action under Title VII”); see also Smith v. Donahoe, No. 11-CV-6243T, 2014 WL 693002, at *7 (W.D.N.Y. Feb. 21, 2014) (“Being asked to undergo a Fitness–for–Duty examination does not constitute a

26
the EEOC has not appropriately clarified that referrals of employees to EAPs or other entities that engage in medical inquiries or examinations constitute prima facie evidence that an employer regards them as having a disability; (3) the EEOC has not appropriately recognized ‘materially adverse’ change in Plaintiff’s employment status [under Title VII] and therefore does not amount to an adverse employment action.”); Tcheskidova v. ITT Federal Services, 2008 WL 3085694 (D. Md. 2008) (claim that mandated psychological fitness-for-duty evaluation violated Title VII failed because the few courts that had considered whether an investigation, by itself, could constitute an adverse employment action had answered that question in the negative).

A few Title VII cases have held that such referrals do constitute adverse employment actions for the purposes of establishing a retaliation claim, see Baur v. Crum, 882 F. Supp. 2d 785, 803, 805 (E.D. Pa. 2012) (defining "adverse employment action" under Title VII as that which a reasonable employee would have found "materially adverse" or an action which well might have dissuaded her from "making or supporting a charge of discrimination." The court concluded that both the mandatory psychological examination at the State EAP and the termination were adverse actions); Ramsey v. New York City Health & Hosps. Corp., No. 98CIV.1594(RPP), 2000 WL 713045, at *12 (S.D.N.Y. June 2, 2000) (considered the order that the worker submit to a psychiatric examination to be an adverse employment action under Title VII.)

For ADA cases holding that such referrals do not constitute adverse employment actions, see Jenkins v. Med. Labs. of E. Iowa, Inc., 880 F.Supp.2d 946, 961 (N.D.Iowa 2012) (a requirement to attend EAP counseling does not constitute a “tangible change in working conditions that produces a material employment disadvantage” under the ADA); Farina v. Branford Bd. of Educ., 458 F. App'x 13, 17 (2d Cir. 2011) (holding that there was no proof that this mandated psychological evaluation had any effect on the terms and conditions of employee’s employment.) (citations omitted); Forgione v. City of New York, No. 11-CV-5248, 2012 WL 4049832, at *5 (E.D.N.Y. Sept. 13, 2012) (employee’s “two referrals for psychological evaluation do not amount to adverse action under the ADA. Although [employee] may have perceived the referrals as inconvenient and unwarranted, and although they may have carried negative connotations, they did not effect a materially adverse change in his working conditions” such as “termination of employment, a demotion evidenced by a decrease in wage or salary, a less distinguished title, a material loss of benefits, [and] significantly diminished material responsibilities”) (citations omitted); Pena v. City of Flushing, 651 F. App’x 415, 422 (6th Cir. 2016) (employer had valid reasons for mandating psychological exam); Dundee v. University Hospitals Corp, No. 1:19-cv-1141, WL 4198891, at *2 (N.D. Ohio July 22, 2020) (referral to EAP not adverse action); see also 2 Americans with Disab.: Pract. & Compliance Manual § 7:185 (Aug. 2021) (claiming that “being required to attend employee assistance program (EAP) counseling” “do[es] not constitute [an] adverse employment actions” and citing Jenkins, 880 F. Supp. 2d 946).

For the sole ADA case I am aware of holding that such referrals do constitute adverse employment actions, see Butler v. State, Louisiana Dept of Pub. Safety & Corr., No. CIVA. 12-00420-BAJ-, 2014 WL 6959940, at *11 (M.D. La. Dec. 4, 2014) (This language is broad enough to encompass the actions Plaintiff has alleged. See 29 C.F.R. § 1630.4(a)(2) (“The term discrimination includes, but is not limited to, the acts described in §§ 1630.4 through 1630.14 of this part); 29 C.F.R. § 1630.13 (“[I]t is unlawful for a covered entity to require a medical examination of an employee or to make inquiries as to whether an employee is an individual with a disability”); 29 C.F.R. § 1630.7 (use of “standards, criteria, or methods of administration which are not job-related and consistent with business necessity” are unlawful); 29 C.F.R. § 1630.12 (retaliation, coercion, interference or intimidation are unlawful). See also Interpretive Guidance to 29 C.F.R. § 1630.5 (“[I]t would be a violation … for an employer to limit the duties of an employee with a disability based on a presumption … about the abilities of an individual with such a disability.”) (emphases added)

EAPs or other entities engaging in medical inquiries or examinations on employers’ behalf as agents of the employer\(^\text{108}\); (4) the provision itself generally has no teeth for current employees, despite the fact that it protects all employees\(^\text{109}\); (5) very few employees are aware of ADA prohibitions on medical inquiries; and (6) elected officials and administrative officials have actually been encouraging workplace surveillance and referrals to EAPs.

### 2. Greater Intrinsic Privacy, Dignitary Harms of Disability-Related Inquiries/Examinations

Both medical inquiries/examinations and big data analytics may result in *extrinsic privacy harms*, or negative consequences, such as discrimination, flowing from acquisition of protected information. Medical inquiries/examinations, however, often result in *intrinsic privacy harms* from the employee’s loss of autonomy and feelings of control over the information and assumptions made about her.\(^\text{110}\) Big data analytics, on the other hand, are less likely to result in such harms when the privacy intrusions occur outside employees’ awareness.

### 3. More Paternalistic Justifications for Disability-Related Inquiries/Examinations

The harms imposed by medical inquiries/examinations seem to appear less obvious to policy-makers than the harms imposed by big data collection and automated electronic surveillance. This may be in part because big data collection and use is less often rationalized as

On the other hand, a referral to an EAP in combination with other relevant evidence could raise an inference that the employer regarded the person as having a substantially limiting impairment. See Holihan v. Lucky Stores, Inc., 87 F.3d 362 (9th Cir. 1996), cert. denied, 520 U.S. 1162 (1997) (reasonable jury could infer that employee was regarded as having a substantially limiting impairment where employer held two meetings to discuss employee's behavior, asked employee if he was having any problems, strongly encouraged employee to seek counseling through EAP, and received several doctors' reports diagnosing employee's depression, anxiety, and stress).

The discussion letter was written, however, prior to the ADA Amendments Act’s reformulation making it easier for employees to establish they are “regarded” as having a disability, as employees referred to EAPs conducting medical inquiries or examinations no longer need to establish that their employers regarded them as having a *substantially limiting* impairment. The appropriate question is whether the EAPs conduct medical inquiries or examinations. And while employers may characterize the reasons for referring people to EAPs as "grief or marriage counseling," the reality is that in-person interactions lasting just a few minutes may be sufficient for mental health providers to infer the presence of a mental disorder. See Andres Herran, Dierdre Sierra-Biddle, Ana De Santiago, Jesús A. Artal, José Luis Vázquez-Barquero & Juan Francisco Diez-Manrique, *Diagnostic Accuracy in the First 5 Min of a Psychiatric Interview: Impact of the Information Given by Patients*, 70 PSYCHOTHERAPY & PSYCHOSOMATICS 141, 141 (2001).

\(^{108}\) U.S. EQUAL EMPLOYMENT OPPORTUNITY COMM’N, *Informal Discussion Letter on ADA: Direct Threat - Confidentiality of Medical Information - Lying on an EEOC Document* (last modified Aug. 23, 2007), https://www.eeoc.gov/foia/eeoc-informal-discussion-letter-164 ("Because the EAP does not act ‘for or on behalf of the employer’ and has no ability to affect employment decisions, Title I of the ADA would likely not govern its activities. Any disclosure that an EAP manager or counselor makes to an employer would be subject to whatever legal, medical, and/or ethical standards regulate the manager's or counselor's work").

\(^{109}\) See, e.g., SAMUEL A. BAGENSTOS, *DISABILITY RIGHTS LAW: CASES AND MATERIALS* 168 (3d ed. 2021) (asking “What damages would an applicant or employee have if she were subjected to a medical examination that violated these provisions?”); Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 WM. & MARY L. REV. 2097, 2157 (2015) (characterizing ADA prohibitions on medical inquiries “as being unduly permissive post-hiring.”)

\(^{110}\) See Roberts, supra note 109, at 2113-15 for further discussion and distinction between intrinsic and extrinsic privacy harms.
providing targeted employees with benefits, whereas mental health inquiries and exams of current employees, are often justified as providing therapeutic or other benefits to employees, which may detract from their privacy harms.111

Some employees even may not initially recognize their interactions with counselors at EAPs or wellness programs as medical examinations because of their dual role in providing counseling, therapy, or health advice. EAPs, for example, function to provide counseling for substance abuse, grief, or depression, but also in “identifying who is at risk”112 for substance abuse and mental disorders and “assist[ing] the employer in assessing the employee's behavior.”113 In addition, employees may not initially recognize psychological counseling as a medical examination114 or be aware that even in-person interactions lasting just a few minutes may be sufficient for some mental health providers infer psychopathology115 about an employee.

4. Recent Government Support for Surveilling Individuals with Mental Health Conditions and Disabilities Through Disability-Related Inquiries and Why the Resulting Data Collected Will Result in Electronic, Automated Worker Surveillance and Management

Finally, it must be observed that recent support for legislation authorizing billions of dollars to collect data, conduct research, and implement programs effecting surveillance of individuals with actual or perceived mental health conditions and disabilities in the workplace (e.g., “encouraging [employees] to seek support and treatment for their own mental health and substance use concerns; and help[ing] such [employees] to identify risk factors in themselves and others and respond to such risks”116) and in educational settings (e.g., the “Federal Clearinghouse on School Safety Evidence-[B]ased Practices,”117 “school threat assessment and intervention

111 In Kroll v. White Lake Ambulance Authority, 763 F.3d 619, 621 (6th Cir. 2014), for example, an employer who reported he decided to compel counseling of an employee having an affair with a peer employee because he thought her “life was a mess and he thought he could help her.” In Schnake v. Johnson County Community College, 961 F. Supp. 1478, 1483 (D. Kan. 1997), the college stated it required an employee to undergo a mental health exam at its Employee Assistance Program because “in it wanted to confirm ‘that it was doing all it could for its employee.’”
112 See David Weiss, Employee Assistance Programs and Behavioral Health Disability, in HANDBOOK OF BEHAVIORAL HEALTH DISABILITY MANAGEMENT 289, 304 (Pamela A. Warren ed., 2018)
113 See id. at 298. Management consultant David Weiss reports that EAPs provide training to "managers and supervisors to facilitate making decisions about whether to seek and when to refer an employee to the EAP." They also play a key role in fitness-for-duty evaluations (FFD) by "assist[ing] the employer in assessing the employee's behavior." "As EAPs have become more sophisticated, coupled with employers becoming more concerned about impairment in the workplace, FFD referrals now not only include drugs/alcohol assessment but now also include the screening for psychiatric and neurological disorders."

Note that there some ambiguity as to when EAP referrals are voluntary or involuntary. For example, Weiss reports that, "A supervisory referral is generally not a mandatory referral to the EAP. However, the supervisor may indicate that EAP involvement is strongly encouraged. Yet, the referral itself is still voluntary." EAPs also "[o]btain the appropriate signed releases from the employee to update the employer of compliance with the referral. In some instance, this type of referral is not considered a mandatory referral."
114 See Kroll v. White Lake Ambulance Authority, 691 F.3d 809, 818-19 (6th Cir. 2012) (holding psychological counseling constituted a medical exam for the purposes of the ADA.)
115 See Andres Herran, Deirdre Sierra-Biddle, Ana de Santiago, Jesus Artal, Juan Francisco Diaz-Manrique & Jose Luis Vazquez-Barquero, Diagnostic Accuracy in the First 5 Min of a Psychiatric Interview: Impact of the Information Given by Patients, 70 PSYCHOTHERAPY & PSYCHOSOMATICS 141, 141 (2001).
teams”\textsuperscript{118}; to “improve the identification and treatment for [adult] students at risk”\textsuperscript{119}; see APPENDIX I) all but guarantees the development of more covert, automated, and electronic systems to surveil these workers in the future. Automated, and electronic systems may result from data collected pursuant to or as an indirect result of this legislation.

Perhaps most problematically, federal government support for these surveillance practices lends these activities and tools great legitimacy. It sends an unmistakable message of approval for surveilling individuals with mental health conditions and disabilities in the workplace. It tells employers, the public, and individuals with mental health conditions and disabilities, that they are dangerous, deficient, dependent on mental health treatment that are not receiving as a result of denial and poor insight, and need to be watched by their employers and their peer coworkers both for their own good and everyone else’s. In sum, federal government support for these mental health awareness activities enhances the discriminatory punch of other surveillance activities.

B. SELECT MEDICAL (DISABILITY-RELATED) INQUIRY/EXAMINATION CASE HISTORY AND DISCUSSION OF THEIR FUNCTIONS

To appreciate the harms of mental health surveillance in the workplace, it is worth reviewing the functions of medical inquiries and examinations for employers, as revealed in case histories.

1. FUNCTIONING TO SUPPRESS RACE, NATIONAL ORIGIN, RELIGION, AND SEX DISCRIMINATION AND RETALIATION CLAIMS

Many Title VII employment discrimination cases reveal employees’ expressions of distress or opposition to discrimination on the basis of race,\textsuperscript{120} national origin,\textsuperscript{121} religion,\textsuperscript{122} or sex,\textsuperscript{123} being cited by employers as justifications for mandated psychiatric evaluations at EAPs


\textsuperscript{120} Lamar v. Alabama Dep't of Conservation & Nat. Res., No. 1:14-CV-571-MHT-PWG, 2016 WL 8814808, at *15 (M.D. Ala. July 26, 2016) (employees alleged that their “attempts to object to [racially] discriminatory conduct were met with open hostility, drug testing, medical inquiries and EAP counseling”); Rogers v. Henry Ford Health Sys., 897 F.3d 763, 766, 776 (6th Cir. 2018) (an African-American woman employed by defendant for over thirty years complained of racial and age discrimination. A few months later, “co-workers began reporting that [her] emotional state was erratic and that they feared she might pose a physical threat to herself or others. In response, [she] was placed on paid leave and sent for a [psychiatric] fitness-for-duty exam” at an EAP).

\textsuperscript{121} Booth v. Pasco Cty., Fla., 757 F.3d 1198, 1198, 1205, 1207 (11th Cir. 2014) (held that the county had “subjected workers to [psychiatric] fitness-for-duty examinations in retaliation for their grievance” of national origin and religious discrimination. The referring supervisor “said that some of the concerns [these employees] expressed in the affidavits were ‘preposterous’ and ‘paranoid,’ [and h]e questioned whether [they] possessed the ‘clear mind’ and focus necessary to protect public safety”).

\textsuperscript{122} Garcia v. Illinois Dep't of Childrern & Fam. Servs., No. 04 C 3906, 2006 WL 2632919, at *12 (N.D. Ill. Sept. 11, 2006) (an employee described being “told by supervisors to stop performing the sign of the cross and to stop saying ‘bendito,’ [and cited a regional supervisor’s] acknowledgments that her performance of the sign of the cross was one of the reasons she was required to undergo a [psychiatric] fitness-for-duty examination” at an EAP)

\textsuperscript{123} Baur v. Crum, 882 F. Supp. 2d 785, 791 (E.D. Pa. 2012) (an employee reported to a human resource analyst that she feared that her supervisor would push down the stairs and that four other coworkers had attempted to physically
and other adverse employment actions that could also be characterized as discrimination on the basis of disability. A familiar pattern emerges from these mandated psychiatric evaluation cases. In Bustillo-Formoso v. Million Air San Juan Corp., for example, a pilot “requested compensation for damages, suffering, and ‘mental anguish’” resulting from age discrimination. In response, the employer cited pilot’s reported “mental anguish” as “extremely serious and worrisome … [for the] safety of [the] passengers,” and mandated the pilot undergo a psychiatric examination. In Osusu-Ansah v. Coca-Cola Co., a call center employee who “worked from home” complained in a meeting with his boss that “managers and employees had discriminated against him or harassed him because he was from Ghana.” He was subsequently asked to speak to “Dr. Marcus McElhaney, Ph.D., an independent consulting psychologist who specialized in crisis management and threat assessment.” Mr. Owusu–Ansah discussed his concerns and described the alleged instances of discrimination. After this meeting, Dr. McElhaney expressed concern to Coca-Cola over the emotional and psychological stability of Mr. Owusu–Ansah, noting that there was a “strong possibility that he was delusional,” and “recommended that Mr. Owusu–Ansah undergo a psychiatric/psychological fitness-for-duty evaluation.”

2. Functioning to Control Women and Their Private Sexual Lives

Cases brought under the ADA also reveal mandated psychiatric evaluations at EAPs functioning to control women and to intrude into their private sexual lives. In one of the most famous of these, Kroll v. White Lake Ambulance Authority, an employer reported he decided to compel counseling (arranged through an EAP) of an employee having an affair with a peer employee because he thought her “life was a mess and he thought he could help her.” He reported he “never had a problem with [her] as far as patient care”; rather, “his primary concerns regarding [the employee] related to her personal life and her sexual relationships.” In Conrad v. Board of Johnson City Commissioners, a nurse practitioner complained of overwork and was required to undergo a fitness-for-duty evaluation formally through her employer’s EAP that inquired into sexual matters, sexual deviancy, threatened assault. The court held the inquiries

_choke/strangle her. She was instructed to contact the State EAP to schedule an independent psychological examination. The court held that the employer easily met its burden to articulate legitimate, nondiscriminatory reasons for instructing the employee to schedule the psychological evaluation—concern for the employee’s “well-being” after she reported her perception of numerous strangulation attempts and a physical fear of her supervisor._

124 Bustillo-Formoso v. Million Air San Juan Corp., 261 F. Supp. 3d 201, 206 (D.P.R. 2016), aff'd, 691 F. App'x 1 (1st Cir. 2017)
125 See id. at 205.
126 Osusu-Ansah v. Coca-Cola Co., 715 F.3d 1306, 1308 (11th Cir. 2013) (“worked from home but was still required to report to the call center for certain meetings”)
127 Id. at 1309.
128 Id.
129 Id.
130 Id.
131 Id. at 1309-10. The court held that the employer’s required evaluation with the Minnesota Multiphasic Personality Inventory (MMPI) was “job-related and consistent with business necessity.” Id. at 1311-12.
133 Id. at 621.
134 Id.
not covered by ADA and that inquiries relating to ‘threatened assault’ were job-related as were relevant to whether the nurse posed a risk to her coworkers given her behaviors. In Baur v. Crum, an employee reported to a human resource analyst that she feared that her supervisor would push her down the stairs and that four other coworkers had attempted to physically choke/strangle her. She was instructed to contact the State EAP to schedule an independent psychological examination. The court held that the employer easily met its burden to articulate legitimate, nondiscriminatory reasons for instructing the employee to schedule the psychological evaluation—concern for the employee's “well-being” after she reported her perception of numerous strangulation attempts and a physical fear of her supervisor.

3. Functioning Otherwise to Justify Control and Adverse Employment Actions Against Workers Under the Guise of Paternalism and Caring

Medical inquiries/examinations often serve to control employees and to justify adverse employment actions under the guise of paternalism and caring. In Schnake v. Johnson County Community College, for example, a college stated it required an employee to undergo a mental health exam at its EAP because “it wanted to confirm ‘that it was doing all it could for its employee.’” In Pickens v. Shinseki, an employee alleged that his employer requested a mental health exam not “because they thought I was disabled, it was just that you have to have some sort of documents to justify firing a guy.”

4. Functioning for More Obviously Overt Punitive and Malicious Purposes

Other cases have also tellingly revealed punitive and malicious, purposes. In Roberts v. Rayonier, Inc., for example, a supervisor referring his employee for a psychiatric examination allegedly stated to him: “boy am I going to have fun with you. I’m going to have you scheduled and find out what makes you tick.”

5. Functioning to Collect Data, Create Algorithmic Workplace Discrimination Tools, and Facilitate Age/Disability Discrimination—EEOC v. Yale New Haven Hospital, Inc

I have previously described how in the buildup to Sections 2703-05 of the American Rescue Plan Act of 2021 and the Dr. Lorna Breen Health Care Provider Protection Act of 2022, hospitals and academic health centers illegally conducted medical inquiries and examinations on health professional employees that built support for this legislation, populated algorithmic scales such as a Physician Well-Being Index and Nurse Well-Being Index, at a profit for the Mayo Clinic, via research supported by federal funds.

138 Id. at 1483.
140 Id. at *10.
141 Roberts v. Rayonier, Inc., 135 F. App'x 351 (11th Cir. 2005).
142 Id. at 353.
143 See generally Nicholas D. Lawson, supra note 18, at 24-26 (“Much of this research has involved questions that constitute medical examinations and that appear to violate the Americans with Disabilities Act. Under the ADA, an employer (and his or her agents) may make medical inquiries or request medical examinations from an employee only for the purposes of determining the ‘ability of an employee to perform job-related functions,’ and this
health professional employees in apparent violation of ADA rules prohibiting medical inquiries and examinations of employees, who are, for example, being “asked to use a brain sensing wearable device (MUSE-S™) on a daily basis to reduce [their] stress”\(^\text{144}\) and having “[s]alivary and hair cortisol and urinary oxytocin collected”\(^\text{145}\) on a regular basis.

Because President Biden and the Senate HELP Committee Chair are both over 80; because both the Senate HELP Committee’s Chair and Ranking Member are 65; because 29% (6/21) of the Senate HELP Committee’s Members are over 70, and 62% (13/21) are over 65,\(^\text{146}\) and because of recent attention to presidential age and competency testing,\(^\text{147}\) it is worth reviewing the ongoing case of \textit{EEOC v. Yale New Haven Hospital, Inc.} As a condition of employment as a clinical faculty member of the Yale School of Medicine (YSM), Yale New Haven Hospital, Inc., (YNHH) required any individual aged 70 and older who applies for or seeks to renew staff privileges at the hospital to take both neuropsychological examinations,\(^\text{148}\) without any suspicion that their neuropsychological ability may have declined.\(^\text{149}\) The U.S. EEOC charged the hospital with violations of the Age Discrimination in Employment Act (ADEA) and the ADA, by subjecting employees to medical examinations that are not job-related and consistent with business necessity.\(^\text{150}\) It also charged that because YNHH medical staff

information cannot be used for other purposes. It does not matter if the employee consents to the other uses. It does not matter if the data are collected through a third party or if the information remains confidential. There are no exceptions for research. The National Institutes of Health (NIH) Office for Human Research Protections, however, has so far not informed institutions, institutional review boards, investigators, or employees about the ADA’s rules. Accordingly, this research has persisted and continues to appear in high-ranking medical journals


The study is one of many medical experiments that appear to have been conducted illegally on employees who “were currently employed at our healthcare facility as HCP (physicians or nurse practitioners or physician assistants),” \textit{id.} at 2, and included apparently illegal medical inquiries/examinations, with questions such as, “Have you been ever diagnosed and/or treated for depression?” and “Have you ever had a panic attack?” \textit{id.} at 5. “\textit{InteraXon} provided all the MUSE-S™ devices at no cost and Creyos Health provided free access to cognition online testing for all participants,” \textit{id.} at 8, and “this study was reviewed and approved by the Mayo Clinic Institutional Review Board (IRB).” \textit{id.} at 9.

\(^{145}\) Arabella Simpkin Begin, Susan Hata, Lori R. Berkowitz, Franziska Plessow, Elizabeth A. Lawson, Nigel Emptage & Katrina Armstrong, \textit{Biomarkers of Clinician Burnout}, 37 J. GEN. INTERNAL MED. 478, 478-79 (2021) (a medical experiment conducted by Massachusetts General Hospital on its employees in which “[s]alivary and hair cortisol and urinary oxytocin were collected, and perceived burnout (two-item MBI), engagement (Utrecht Work Engagement Scale), connection (‘I feel a strong sense of connection and community at work’), and trust (‘I trust my obgyn colleagues and feel safe discussing concerns with them’) were measured in 25 female clinicians in the ObGyn Department at MGH”; one author “is on the scientific advisory board and has a financial interest in OXT Therapeutics, a company developing an intranasal oxytocin and long-acting analogs of oxytocin to treat obesity and metabolic disease”)

\(^{146}\) Bernie Sanders (81); Patty Murray (72); Tim Kaine (65); Maggie Hassan (65); Tina Smith (65); John Hickenlooper, Jr. (71); Ed Markey (76); Bill Cassidy (65); Susan Collins (70); Lisa Murkowski (65); Mike Braun (69); Mitt Romney (76); Tommy Tuberville (68).


\(^{149}\) \textit{id.} at 7.

\(^{150}\) \textit{id.}
privileges are a condition of employment as a clinical faculty member of the YSM, the policy interferes with the enjoyment of rights protected under the ADA of YSM employees.\textsuperscript{151}

In addition, “[m]ultiple [YNHH/YSM] employees’ test results were anonymously published in a Jan[uary] 14 paper in the Journal of the American Medical Association” \textsuperscript{152} (JAMA). “One of the doctor[s] — who asked to remain anonymous to avoid retaliation by the hospital — said … that they were never asked for consent to use their test results in the Jan[uary] 14 paper.” The authors claimed, however, that “no action was taken that was not voluntary.”\textsuperscript{153}

The authors claimed that their screening and neuropsychological tools identified 18 individuals (out of 141 [12.5%]) who they believed had “cognitive deficits that were likely to impair their ability to practice medicine independently.”\textsuperscript{154} The authors also warned that, “[n]one of these 18 clinicians had previously been brought to the attention of medical staff leadership because of performance problems.”\textsuperscript{155} Though the authors apparently interpreted these results as proof that their screening battery was very good at identifying physician-accidents waiting to happen, the results in fact seem to suggest the opposite—that their screenings had a 100% false positive rate, “detecting” physicians with no performance problems 100% of the time. One of the four JAMA articles written about the study on January 14 acknowledged that “little is known about the accuracy of these assessments in predicting a clinician’s subsequent quality of care or patient outcomes.”\textsuperscript{156} But \textit{all four} recommended conducting even more similar research, data collection, medical inquiries and examinations for cognitive impairment.\textsuperscript{157}

As I have described elsewhere,\textsuperscript{158} this research conducted on health professionals involves questions that constitute medical inquiries or examinations and violate the ADA. Under the ADA, an employer (and his or her agents) may make medical inquiries or request medical

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{151} Id. at 8.
\item \textsuperscript{153} Cooney & Balcezak, \textit{supra} note 152, at 180.
\item \textsuperscript{154} Id.
\item \textsuperscript{155} Id.
\item \textsuperscript{156} Katrina A. Armstrong & Eileen E. Reynolds, \textit{Opportunities and Challenges in Valuing and Evaluating Aging Physicians}, 323 [J]AMA 125, 125 (2020).
\item \textsuperscript{157} See id. at 126 (admitting that the Age Discrimination in Employment Act “substantially limit[s] the ability of organizations that employ physicians to implement age-based screening” but endorsing screening nevertheless through “a multistep process”); Cooney & Balcezak, \textit{supra} note 152, at 126; Sally A. Santen, Robin R. Hemphill & Martin Pusic, \textit{The Responsibility of Physician to Maintain Competency}, 323 [J]AMA 117 (2020) (reporting that testing is particularly needed because “for a physician to be able to admit that he or she is not competent in something is a loss of self”); Jeffrey L. Saver, \textit{Best Practices in Assessing Aging Physicians for Professional Competency}, 323 [J]AMA 127, 128 (2020) (“Nuanced, supportive, evidence-based programs can help ensure that patients are protected from late-career physicians who become affected by cognitive decline”).
\item Proponents of cognitive screening research presenting themselves as doing older physicians a favor—arguing that cognitive screening research is inevitable, and at least \textit{their} screening/termination algorithms might be fairer and at least better than mandatory retirement policies. \textit{See} Am. Med. Ass’n, Council on Med. Educ., \textit{Competency of Senior Physicians}, at 9 (Jan. 1, 2018), https://downloads.aap.org/DOSP/SeniorPhysiciansCompetency.pdf (“It is critical that physicians take the lead in developing standards for monitoring and assessing their personal competency and that of fellow physicians to head off a call for nationally implemented mandatory retirement ages or imposition of guidelines by others.”)
\item \textsuperscript{158} Lawson, \textit{supra} note 18, at 25.
\end{itemize}
\end{footnotesize}
examinations from an employee only for the purposes of determining the “ability of an employee to perform job-related functions,” and this information cannot be used for other purposes.\textsuperscript{159} It does not matter if the employee consents to the other uses. It does not matter if the data are collected through a third party or if the information remains confidential. There are no exceptions for research. The HHS Office for Human Research Protections and National Institutes of Health, however, have so far not informed institutions conducting research, institutional review boards, investigators, or employees about the ADA’s rules.\textsuperscript{160} Accordingly, this research has persisted and continues to appear in high-ranking medical journals.\textsuperscript{161}

IV. RESPONSES TO SPECIFIC REQUEST FOR INFORMATION QUESTIONS

c. The type of automated surveillance or management you have experienced, including the location of the monitoring technology (such as an app you had to use or download; a device you had to use, carry, or wear; or a camera that monitors you);

I have no personal experience with electronic/technological surveillance as a worker.

e. Whether and when your employer informed you about their use of automated worker surveillance and management systems;

f. Whether you (or, if relevant, your representative, like a labor union) have any input or control over how, where, and over what automated surveillance occurs;

No. In my personal experiences as an employee (i.e., as a psychiatry resident), my employers’ requests to me to undergo psychiatric/psychological evaluations, provide unfettered access to my mental health information, and see the providers chosen by my employers, were not optional. Nor were they optional for the 20% of the other residents in my first program, who were required to do the same.

Being the subject of workplace-wide and peer-to-peer surveillance is also not optional for the health professionals and students with mental health conditions and disabilities who are subjected to these mental health awareness activities.

g. Whether you know how the data generated by surveillance is used for management or other purposes (including purposes related to employment or labor market competition);

Yes. See above description of the Physician Well-Being Index, Nurse Well-Being Index, the neuropsychological testing instruments in \textit{EEOC v. Yale New Haven Hospital, Inc.}, the description of student surveillance through Federal Clearinghouse on School Safety Evidence-

\textsuperscript{159} 29 C.F.R. § 1630.14(c).


\textsuperscript{161} See, e.g., supra notes 153-57 and accompanying discussion.
Based Practices, threat assessments, Project AWARE, mental health awareness training, and other programs described in APPENDIX I.

**h. Whether you (or, if relevant, your representative, like a labor union) have any visibility into the data collected on you or how it is used, including whether data on you collected by surveillance can be shared with other companies, trade groups, or third parties;**

**i. How automated surveillance and management systems have affected your workplace rights, including rights around collective action, labor organizing, collective bargaining, pay, reasonable accommodations, health and safety, discrimination, and harassment—or your expectation of retaliation when exercising these rights;**

Yes (regarding question h). See above description of the Physician Well-Being Index, Nurse Well-Being Index, the neuropsychological testing instruments at issue in *EEOC v. Yale New Haven Hospital, Inc.*, and used by Mayo Clinic and Yale New Haven Hospital, Inc.

The U.S. HHS leaders, such as Secretary Xavier Becerra and Surgeon General Vivek Murthy, hospitals, professional medical associations, and other health businesses that lobbied for the Dr. Lorna Breen Health Care Provider Protection Act\(^\text{162}\) may have achieved, or come close to

---

achieving, a way to formally undermine and circumvent workers’ rights under the ADA to be free from unwarranted disability-related inquiries and requests for medical examinations.

As the EEOC has explained, “[a]n employer may make disability-related inquiries and require employees to submit to medical examinations that are mandated or necessitated by another federal law or regulation.” Those seeking to engage in otherwise ADA-prohibited inquiries and examinations may be able to argue that they are necessitated by, for example, the Dr. Lorna Breen Health Care Provider Protection Act.

It is also likely that HHS will use the hundreds of millions of dollars appropriated to HHS to collect data and create bogus “best practices,” “recommendations,” a bogus “national evidence-based or evidence-informed education and awareness initiative[s],” based on a bogus HHS “review on improving health care professional mental health” and the “efficacy of health professional training programs that promote resiliency and improve mental health”—to argue that health professionals with mental health conditions and disabilities are so dangerous, and their initiative and programs so effective, that

(1) mental health inquiries and examinations of health professionals must be mandated or necessitated by a new federal law or regulation; or that

(2) health professionals must be considered “employees in positions affecting public safety” for whom periodic mental health examinations are “necessary to determine whether [they] currently [are] unable to perform [their] essential job functions or pose[] a direct threat due to the[ir] condition.”

---

163 U.S. EQUAL EMPLOYMENT OPPORTUNITY COMM’N, supra note 87 (“For example, under federal safety regulations, interstate bus and truck drivers must undergo medical examinations at least once every two years. Similarly, airline pilots and flight attendants must continually meet certain medical requirements. Other federal laws that require medical examinations or medical inquiries of employees without violating the ADA include: the Occupational Safety and Health Act; the Federal Mine Health and Safety Act; and other federal statutes that require employees exposed to toxic or hazardous substances to be medically monitored at specific intervals.”) (citations omitted)

164 Dr. Lorna Breen Health Care Provider Protection Act, Pub. L. No. 117–105, § 2, 136 Stat. 1118, 1118 (2022) (“Not later than 2 years after the date of the enactment of this Act, the Secretary of Health and Human Services (referred to in this Act as the ‘Secretary’) shall identify and disseminate evidence-based or evidence-informed best practices for preventing suicide and improving mental health and resiliency among health care professionals, and for training health care professionals in appropriate strategies to promote their mental health. Such best practices shall include recommendations related to preventing suicide and improving mental health and resiliency among health care professionals.”)

165 Id.

166 Id. (“The Secretary, in consultation with relevant stakeholders, including medical professional associations, shall establish a national evidence-based or evidence-informed education and awareness initiative— (1) to encourage health care professionals to seek support and care for their mental health or substance use concerns, to help such professionals identify risk factors associated with suicide and mental health conditions, and to help such professionals learn how best to respond to such risks, with the goal of preventing suicide, mental health conditions, and substance use disorders”)

167 See generally U.S. EQUAL EMPLOYMENT OPPORTUNITY COMM’N, supra note 87 (“May employers require periodic medical examinations of employees in positions affecting public safety (e.g., police officers and firefighters)? Yes. In limited circumstances, periodic medical examinations of employees in positions affecting public safety that are narrowly tailored to address specific job-related concerns are permissible.”). Responding to Nicholas D. Lawson, Physician Burnout and the Americans with Disabilities Act, 50 HASTINGS CTR. REP. 47 (2020),
There is a long history of efforts to exclude senior physicians and physicians with mental health conditions and subject them to medical inquiries and examinations on the false grounds that physicians occupy positions of public safety. Owners of addiction businesses targeting lawyers have also argued that lawyers occupy positions of public safety for similar reasons.\textsuperscript{168}

Current U.S. HHS General Counsel Samuel Bagenstos has described how “industry-specific agencies are most likely to be responsive to the concerns of the industry, labor union, and public interest groups”\textsuperscript{169} and observed that when “the regulations adopted by industry-specific or subject-matter-specific regulatory agencies displace the ADA’s direct threat requirement, [this] might encourage businesses to seek the promulgation of such regulations as a shield against ADA liability.”\textsuperscript{170}

\textit{j. Whether your employer has used information from an automated surveillance and management system in support of any discipline against you—and if so, what the action was, how and when you were informed, and what information was provided to you or your representative (such as a labor union);}

At both psychiatry residency programs where I was employed, my program directors cited my reluctance or resistance to submitted to their requests that I submit to mental health

\begin{flushleft}
Sharona Hoffman, \textit{Sharona Hoffman Replies}, 50 HASTINGS CTR. REP. 47, 47 (2020) states, “employers may require periodic job-related medical examinations of all employees ‘in positions affecting public safety.’ As I argued in my commentary, doctors, to whom patients entrust their health every day, have safety-critical jobs.” Yet as Ilene Moore observes, “any interpretation suggesting that physicians are in a position affecting public safety is not supported by the statutory language of the ADA, the EEOC Enforcement Guidance, or EEOC correspondence. Only one federal law defines some physicians as public safety officers: physicians who serve as part of a public rescue squad or ambulance as def...” Ilene N. Moore, \textit{Screening Older Physicians for Cognitive Impairment: Justifiable or Discriminatory}, 28 HEALTH MATRIX 95, 140 (2018) (internal citations omitted).
\end{flushleft}

\begin{flushleft}
\textsuperscript{168} When I interned at the American Bar Association Commission on Disability Rights after my first year of law school, Link Christin, Executive Director of a legal professionals program, was trying to get the Commission to publish a book warning: “The argument can be made that the work of attorneys is life and death in nature, or at least critical enough that there is NO room for impairment. The work of criminal lawyers concerns the liberty of others, and, in some cases, the lives of others. Estate lawyers are responsible for the planned future of assets, property, and personal property to generations. Family law practitioners influence such emotionally-charged decisions as custody, visitation, alimony, and safety between spouses and families. And the list goes on.”; “The business of attorneys may not have the visceral ramifications of medicine or air flight when mistakes are made, but the addiction-induced errors of attorneys can have a profound impact on individuals and businesses alike.”; “The profound dangers to the attorney, her client, her firm, and her family are only limited by one’s imagination. They can – and do – include complete loss of cognitive functioning, ‘blackouts,’ aggressive behavior, isolation, panic attacks, shutting down, sexual misconduct, criminal activity, dangerous actions, physical damage…. Addiction manifests in behaviors which are typically negative and antisocial … lying, cheating, stealing, hiding, and breaking of trust.”
\end{flushleft}

\begin{flushleft}
\textsuperscript{169} Samuel R. Bagenstos, \textit{Disability and Safety Risks}, in \textit{LAW AND THE CONTRADICTIONS OF THE DISABILITY RIGHTS MOVEMENT} 76, 86 (2009) (describing Albertson’s, Inc., v. Kirkingburg, 529 U.S. 555 (1999) as an example of deference to Federal Highway Administration (FHWA) regulations and how “the exclusive focus on the interests of employers and employees led OSHA [the Occupational Safety and Health Administration] to disregard the interests of—and even encourage discrimination against—people with disabilities.”)
\end{flushleft}

\begin{flushleft}
\textsuperscript{170} Id.; see also Samuel R. Bagenstos, \textit{The Americans with Disabilities Act as Risk Regulation}, 101 COLUM. L. REV. 1479, 1486 (2001) (observing that “[l]ong experience has led disability rights activists to look with suspicion on the so-called ‘experts,’” and that professionals’ responses to disability “principally serve the interests of the professionals themselves, by creating a class of disabled people who must turn to the professionals for help.”)
\end{flushleft}
examinations and be followed by a psychologist as reasons for me to be fired. At my first program, my resistance to submitting to these processes was cited by members of my hospital’s internal appeals panel, and I was in the room when my program director at my second program brought this up as a reason for my termination. At my first program, the other residents, including myself, who were required to provide our program directors unfettered access to mental health evaluations and see the providers chosen by them were individuals who had been critical of the program.

See above case history on medical inquiries/examinations “Functioning to Suppress Discrimination and Retaliation Claims.” I have also written previously on how descriptions of physician impairment problematically include denial (e.g., “denying or expressing guilt or shame about personal use”) or complaining or asserting one’s rights against management (e.g., “involvement in litigation against hospital”), making it harder for all employees to exercise their rights to be free from harassment, discrimination, and retaliation, or to blow the whistle on employers and management.171

n. If you are disabled or have a health condition, how automated surveillance and management systems have impacted or may impact your use of reasonable accommodations; such as assistive technology or accessibility features of software or breaks, or affected your ability to keep information about your condition private from your employer, supervisor, or coworkers;

I have never observed these systems interfering with my use of reasonable accommodations. They absolutely have interfered with my ability to keep information about my condition private from employers, supervisors, and coworkers.

At my second program, for reasons unclear, my program director asked within the first month whether I thought it might be helpful to submit to sessions with a psychologist he described as a “professional job coach.” The program coordinator subsequently warned me that I would be retaliated against if I did not agree. Though I had received all passing, positive evaluations and scored at the top of my class on in-service examinations,172 my program director monitored my attendance with the psychologist, criticized me when the psychologist wanted to end the sessions for lack of need, and later requested a meeting with her in person. The sessions with the psychologist absolutely involved medical inquiries.

The surveillance encouraged by the recent and proposed federal legislation described supra absolutely interfere with the ability of workers with disabilities and health conditions to keep information about their condition private from employers, supervisors, and coworkers.

171 Lawson, supra note 55, at 106-07 (citations omitted).
172 And scored on my Psychiatry Resident In Training Examinations as a PGY 2, in the 98th percentile among all PGY 1-4 psychiatry residents nationally, and 1st among the 16 residents in the program for psychiatry questions, and in the 89th percentile among all PGY 1-4 psychiatry residents nationally, and also 1st among the 16 residents in the program for neurology questions; as a PGY 1, in the 95th percentile among all PGY 1 psychiatry residents nationally, and 1st among the 7 in my residency program class year for psychiatry questions, and in the 99th percentile among all PGY 1 psychiatry residents nationally, and also 1st among the 7 in my residency program class year for neurology questions.
The federal statutes, programs, and guidance encouraging surveillance of individuals with mental health conditions and the surveillance activities themselves are perhaps most problematic for the ableist stigma and prejudice they engender. They tell employers, the public, and individuals with mental health conditions and disabilities, that they are dangerous, deficient, dependent on mental health treatment that they are not receiving as a result of denial and poor insight, and need to be watched by their employers and their peer coworkers both for their own good and everyone else’s. They all-but guarantee that workers with mental health conditions will be excluded, discriminated against, and treated unfairly by employers and management at their jobs.

How does it make me feel to see progressive elected officials, in the 2022 elections, intentionally campaign on surveillance legislation that “inappropriately scapegoat[s] people with mental health disabilities, and further[s] racial disparities,”\(^{173}\) and “inappropriately links mental health, and the need for mental health services, to gun violence”\(^{174}\)? How does it make me feel to see the Biden administration, Members of Congress, and institutions focus exclusively on surveilling people with mental health conditions, and never on including them? It makes me angry. It makes me want to protest and hold those accountable for facilitating this surveillance. I have personally found the economic and health effects of this surveillance to be negative.

V. RECOMMENDATIONS

A. REPEAL OR AT LEAST STOP FUNDING FEDERAL GRANT PROGRAMS THAT ENCOURAGE SURVEILLANCE AND MANAGEMENT OF INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

The Biden administration and Congress should eliminate the provisions of the Dr. Lorna Breen Health Care Provider Protection Act codified in 42 U.S.C. § 294t and should stop funding for these provisions as soon as possible. They should not pass the Supporting the Mental Health of Educators and Staff Act of 2023, the Providing Resources and Occupational Training for


\(^{174}\) Bazelon Ctr. for Mental Health Law, *supra* note 34, at 3 (regarding the Bipartisan Safer Communities Act, which was supported by every Democratic Member of Congress).
Emotional Crisis and Trauma (PROTECT) in 911 Act, or the DHS Suicide Prevention and Resiliency for Law Enforcement Act.

Though prohibited medical inquiries and examinations may be better handled by the EEOC’s systemic program than through individual lawsuits, they have become far too ubiquitous for the EEOC to effect meaningful change, especially in the context of recent legislation and other federal government support for surveillance.

The Biden administration and Congress should also eliminate provisions of the U.S.C. described in the APPENDIX I and stop funding for activities (i.e., threat assessments, Project AWARE) that encourage surveillance of students with mental health conditions and disabilities, and students of color.

B. DIRECT FEDERAL GOVERNMENT AGENCIES, INCLUDING THE U.S. HHS, SURGEON GENERAL, AND ODEP, TO STOP ENCOURAGING SURVEILLANCE AND MANAGEMENT OF INDIVIDUALS WITH MENTAL HEALTH CONDITIONS AND DISABILITIES

The guidance and publications described above are unacceptable. It is well within the control of the administration to have them removed and to direct the members of the administration who are disseminating them to no longer do so.

C. DIRECT THE HHS OFFICE OF HUMAN RESEARCH PROTECTIONS TO ISSUE APPROPRIATE GUIDANCE; DO NOT FUND FEDERAL RESEARCH AT INSTITUTIONS THAT ENGAGE IN MEDICAL RESEARCH, INQUIRIES, OR EXAMINATIONS OF EMPLOYEES

The administration should call on Julie Kaneshiro, Acting Director of the HHS Office of Human Research Protections, to issue guidance and explicit directives to all institutions conducting federally funded research, to inform them and their employees about ADA prohibitions on medical inquiries and examinations. The Office should make them aware that these prohibitions apply regardless of any Common Rule regulations on human subjects research (45 C.F.R. § 46 et seq.):

• regardless of whether such inquiries/examinations are characterized as research or as not involving research (e.g., as “quality improvement”);
• regardless of whether such inquiries/examinations are characterized as exempt research under 45 C.F.R. § 46.104;
• regardless of whether employees consent;

175 U.S. Equal Emp’t Opportunity Comm’n, Advancing Opportunity A Review of the Systemic Program of the U.S. Equal Employment Opportunity Commission (July 7, 2016), https://www.eeoc.gov/advancing-opportunity-review-systemic-program-us-equal-employment-opportunity-commission (Figure 3 reporting successful conciliations of systemic investigations by issue (FY2011-2015) as 23% for hiring; 21% for reasonable accommodation; 12% for discharge; 10% for terms and conditions; 8% for medical inquiry/exam; Figure 4 reporting systemic lawsuit resolutions by issue (FY2011-2015) as 25% for hiring; 22% for harassment; 9% for prohibited inquiry/exam)
• regardless of whether the data are collected through a third party or if the information remains confidential

D. INCLUDE PEOPLE WITH DISABILITIES IN HEALTH WORKFORCE INCLUSION STATUTES; ADD DISABILITIES TO THE EEOC’S EEO FORMS; UPDATE SECTION 503 TO ALIGN WITH SECTION 501

A recurrent theme within the legal academy and disability rights discourse is whether disability identification is being used or else serving to include or to exclude.176 Exclusionary disability identifications in the K-12 educational context are most often discussed in relation to the disproportionate labeling of Black children with intellectual disability and serious emotional disturbance under the Individuals with Disabilities Education Act (IDEA).177 I have described previously how mental health identifications in educational settings, particularly in the college/university context, serve to exclude students with actual or perceived mental health conditions and disabilities. The disability identification and surveillance activities I have described in this letter absolutely serve to exclude, rather than include, individuals with mental health conditions.

The most important step the Biden administration can take to stop these exclusionary practices is to stop promoting them. The administration can also take active steps to meaningfully include individuals with mental health conditions by, for example, aligning disability affirmative action requirements for contractors with those that exist for federal employees.178 The administration could also include individuals with mental health conditions

---

176 BAGENSTOS, supra note __, at 66-67 ("Although the IDEA is designed to benefit students with disabilities, there are harms to an erroneous disability identification. ‘It can,’ for example, ‘equate to stigma, lowered educational opportunity, and increased contact with the juvenile justice system.’" (citing Claire Raj, The Misidentification of Children with Disabilities: A Harm with No Foul, 48 ARIZ. ST. L.J. 373, 387 (2016)).
178 See Letter from Disability Rights and Labor Partners to Shalanda Young, Acting Dir., Office of Mgmt. & Budget 2-4 (July 6, 2021), https://secureusercontent.com/wp-content/uploads/2021/07/Disability-and-Labor-Joint-Submission-to-OMB-2021-0005_for-distribution.pdf (“there is no requirement for such contractors to track such data… The Department of Labor’s aspirational goal is both too low for people with all disabilities and omits the important sub-goal for people with significant disabilities who have historically been the most underemployed. The employment positions offered by federal contractors are not radically different from those in the federal government. People with disabilities hold a wide variety of jobs in the federal government, including jobs with management or supervisory responsibilities, jobs that are physically strenuous, and jobs that expose individuals to taxing or hazardous conditions. There is no reason why the goals of Section 501 cannot be extended to Section 503 as well.”); Letter from Consortium for Citizens with Disabilities to Jenny R. Yang, Dir., Office of Fed. Contract Compliance Programs, U.S. Dep’t of Labor, at 3 (May 7, 2021), http://www.c-c-d.org/fichiers/CCD-Ideas-for-OFCCP-2021-FINAL.pdf (“Strengthen the 7% utilization goal by mirroring the EEOC rule on 12%, disaggregate the data and set a separate targeted disability goal, and encourage self-reporting of data without penalty to create a culture of sharing disability data”); Chai Feldblum, Thoughts on Joining the AbilityOne Commission (Aug. 26, 2021), https://www.chaifeldblum.com/thoughts-on-joining-the-abilityone-commission/ (“hope the Department of Labor will modify its Section 503 regulations so that they align with the EEOC’s Section 501 regulations”)
and other disabilities on EEO-1 forms for private employers, EEO-4 forms for state and local governments, EEO-5 forms for elementary and secondary level school districts, and EEO-6/IPEDS forms for institutions of higher education. The federal government could also consider finally including individuals with mental health conditions and other disabilities within federal legislation to bolster diversity within the health professions, such as the Health Professions Education Extension Amendments of 1999, the Health Professions Education Partnerships Act of 1998, and the Patient Protection and Affordable Care Act of 2010. The later also did not include persons with mental health conditions and disabilities as targets of “[m]ental and behavioral health education and training grants.”

Thank you very much for considering these comments, and please contact me with any questions.

Sincerely,

Nicholas D. Lawson, M.D., J.D.

---

179 See DISABILITY & PHILANTHROPY FORUM, Disability Participation: Demographic Tracking and Self-Identification (July 8, 2021), https://disabilityphilanthropy.org/wp-content/uploads/2021/09/Transcript-2021-Journey-to-Inclusion-Series-Disability-Participation-Demographic-Tracking-and-Self-identification-7-8-21.docx ("the EEO-1 form, which asks about gender and race. It does not ask about disability. It does not ask about sexual orientation or LGBTQ status. I and others worked very hard at the [EEOC] commission to argue why the EEO-1 should be changed. It hasn't.")


181 Health Professions Education Partnerships Act of 1998, Pub. L. No. 105-392, § 101, 112 Stat. 3524, 3525 (1998) (codified at 42 U.S.C. § 293; “Centers of excellence”); § 101, 112 Stat. at 3531-3532 (codified at 42 U.S.C. § 293a; “Scholarships for disadvantaged students”); § 101, 112 Stat. at 3534 (codified at 42 U.S.C. § 293b(5); “Loan repayments and fellowships regarding faculty positions”); § 101, 112 Stat. at 3534, 3536 (codified at 42 U.S.C. § 293c; “Educational assistance in the health professions regarding individuals from disadvantaged backgrounds”); § 102, 112 Stat. at 3539 (codified at 42 U.S.C. § 293l(3); “Advisory Committee on Training in Primary Care Medicine and Dentistry”; “the Secretary shall ensure the adequate representation of women and minorities”); § 103, 112 Stat. at 3549 (codified at 42 U.S.C. § 294(b)(3); “Advisory Committee on Interdisciplinary, Community-Based Linkages”; “the Secretary shall ensure the adequate representation of women and minorities”); § 105, 112 Stat. at 3553 (42 U.S.C. § 295(c); “General provisions”); § 106, 112 Stat. at 3558-59 (codified at 42 U.S.C. § 295o-1; “Generally applicable provisions”; “The Secretary shall establish procedures to ensure that, with respect to any data collection required under this title, such data is collected in a manner that takes into account age, sex, race, and ethnicity”; “the Secretary shall ensure sex, racial, ethnic, and geographic balance among the membership” of groups peer reviewing grants for health professions training programs”); § 123, 112 Stat. at 3566 (codified at 42 U.S.C. § 296e(2); “Generally applicable provisions”; “the Secretary shall "ensure sex, racial, ethnic, and geographic representation among the membership" of groups peer reviewing grants for nurse training programs”); § 123, 112 Stat. at 3573 (codified at 42 U.S.C. § 297t(3); “National Advisory Council on Nurse Education and Practice”; “the Secretary shall ensure the adequate representation of minorities.”)


183 § 5306, 124 Stat. at 626 (codified at 42 U.S.C. § 294e-1; “Mental and behavioral health education and training grants”; “To be eligible for a grant under this section, an institution shall demonstrate … (2) participation in the institutions' programs of individuals and groups from different racial, ethnic, cultural, geographic, religious, linguistic, and class backgrounds, and different genders and sexual orientations; (3) knowledge and understanding of the concerns of the individuals and groups described in paragraph (2)”)
## Appendix I. Sections of the U.S.C. Authorizing or Contributing to Mental and Behavioral Health Surveillance in Schools

<table>
<thead>
<tr>
<th>Sections of U.S.C.</th>
<th>Relevant Excerpts from U.S.C. Section</th>
<th>Legislative History</th>
<th>Appropriations</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Matching grant program for school security] Program authorized (34 U.S.C. § 10551)</td>
<td>“Training school personnel and students to prevent student violence against others and self”; “The development and operation of (A) school threat assessment and intervention teams that may include coordination with law enforcement agencies and school personnel; and (B) specialized training for school officials in responding to mental health crises”; “[4]] improvement in training, threat assessments and reporting, and violence prevention. (5) Coordination with local law enforcement. (6) Training for local law enforcement officers to prevent student violence against others and self.”</td>
<td>Bipartisan Safer Communities Act, Pub. L. No. 117-159, 136 Stat. 1313, 1339 (2022) (“for each of fiscal years 2022 through 2026 … $200,000,000 shall be for grants administered by the Bureau of Justice Assistance for purposes authorized under the STOP School Violence Act of 2018 (title V of division S of Public Law 115–141) … For an additional amount for ‘Community Oriented Policing Services Programs’, $100,000,000, to remain available until expended, for competitive grants to be administered by the Community Oriented Policing Services Office for purposes authorized under the STOP School Violence Act of 2018 (title V of division S of Public Law 115–141)”</td>
<td>$200,000,000 for each of fiscal years 2022 through 2026</td>
</tr>
<tr>
<td>[Edward Byrne Memorial Justice Assistance Grant Program] Description (34 U.S.C. § 10152)</td>
<td>“[(a)(1)] (H) Mental health programs and related law enforcement and corrections programs, including behavioral programs and crisis intervention teams. (I) Implementation of State crisis intervention court proceedings and related programs or initiatives, including but not limited to— (i) mental health courts; (ii) drug courts; (iii) veterans courts; and (iv) extreme risk protection order programs…”</td>
<td>ORIGINATED FROM: Helping Families in Mental Health Crisis Reform Act of 2016 (division B of Public Law 114–255), § 14001, 130 Stat. at 1287 (“Section 501(a)(1) of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3751(a)(1)) is amended by adding at the end the following: ‘(H) Mental health programs and related law enforcement and corrections programs, including behavioral programs and crisis intervention teams.’”)</td>
<td>$750,000,000 altogether</td>
</tr>
<tr>
<td></td>
<td>“(h) Annual report on crisis intervention programs The Attorney General shall publish an annual report with respect to grants awarded for crisis intervention programs or initiatives under subsection (a)(1)(I) that contains— (1) a description of the grants awarded and the crisis intervention programs or initiatives funded by the grants, broken down by grant recipient; (2) an evaluation of the effectiveness of the crisis intervention programs or initiatives in preventing violence and suicide; (3) measures that have been taken by each grant recipient to safeguard the constitutional rights of an individual subject to a crisis intervention program or initiative; and (4) efforts that the Attorney General is making, in coordination with the grant recipients, to protect the constitutional rights of individuals subject to the crisis intervention programs or initiatives.”</td>
<td>Bipartisan Safer Communities Act, Pub. L. No. 117-159, § 12003, 136 Stat. 1313, 1325 (2022) (“Section 501(a)(1) of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (34 U.S.C. 10152(a)(1)) is amended— (1) in the matter preceding subparagraph (A), by inserting ‘or civil proceedings’ after ‘criminal justice’; and (2) by adding at the end the following: ‘(I) Implementation of State crisis intervention court proceedings and related programs or initiatives, including but not limited to—(i) mental health courts; (ii) drug courts; (iii) veterans courts; and (iv) extreme risk protection order programs’”)</td>
<td>“for each of fiscal years 2022 through 2026”</td>
</tr>
<tr>
<td>Grants to improve trauma support</td>
<td>“Collaborative efforts between school-based service systems and trauma-informed support and mental health service systems to provide, develop, or administer services to trauma survivors.”</td>
<td>ORIGINATED FROM: Substance Use-Disorder Prevention that Promotes Opioid Recovery and Treatment (SUPPORT) for Patients and Communities Act, Pub. L. No.</td>
<td>“$50,000,000 for each of fiscal years 2022 through 2026”</td>
</tr>
</tbody>
</table>

### Note

- The figures for appropriations reflect the total amount available for each fiscal year, with specific allocations for grants to specific programs. The amounts are inclusive of both federal and state contributions, as well as any additional funds authorized by the Bipartisan Safer Communities Act of 2022. The data is based on the legislative history and appropriations for the relevant sections of the U.S.C., as outlined above.
<p>| services and mental health care for children and youth in educational settings (42 U.S.C. § 280h-7) | improve prevention, screening, referral, and treatment and support services to students, such as providing trauma screenings to identify students in need of specialized support.” “To provide professional development to teachers, teacher assistants, school leaders, specialized instructional support personnel, and mental health professionals that … improves school capacity to identify, refer, and provide services to students in need of trauma support or behavioral health services”; “Engaging families and communities in efforts to increase awareness of child and youth trauma, which may include sharing best practices with law enforcement regarding trauma-informed care and working with mental health professionals to provide interventions” | 115-271, § 4134, 132 Stat. 3894, 4051-55 (2018) (“$50,000,000 for each of fiscal years 2019 through 2023.”) | years 2019 through 2023.” “$28,000,000” “in equal amounts for each of fiscal years 2022 through 2025” |
| Suicide prevention technical assistance center (42 U.S.C. § 290bb–34) | “ensuring the surveillance of suicide early intervention and prevention strategies for all ages, particularly among groups that are at a high risk for suicide”; “further identifying and understanding causes and associated risk factors for suicide”; “ensuring the surveillance of suicidal behaviors and nonfatal suicidal attempts”; “promoting the sharing of data regarding suicide with Federal agencies involved with suicide early intervention and prevention, and State-sponsored statewide or tribal suicide early intervention and prevention strategies for the purpose of identifying previously unknown mental health causes and associated risk factors for suicide” | ORIGINATED FROM: Garrett Lee Smith Memorial Act, Pub. L. No. 108-355, § 3, 118 Stat. 1404, 1405-07 (2004) | “$9,000,000 for each of fiscal years 2023 through 2027” |
| Youth suicide early intervention and prevention strategies (42 U.S.C. § 290bb–36) | “provide early intervention and assessment services, including screening programs, to youth who are at risk for mental or emotional disorders that may lead to a suicide attempt, and that are integrated with school systems, educational institutions, juvenile justice systems, substance use disorder programs, mental health programs, foster care systems, and other children and youth support organizations”; “offer continuous and up-to-date information and awareness campaigns that target parents, family members, child care professionals, community care providers, and the general public and highlight the risk factors associated with youth suicide and the life-saving help and care available from early intervention and prevention services” | ORIGINATED FROM: Garrett Lee Smith Memorial Act, Pub. L. No. 108-355, § 3, 118 Stat. 1404, 1409-13 (2004) (“$7,000,000 for fiscal year 2005, $18,000,000 for fiscal year 2006, and $30,000,000 for fiscal year 2007”) | “$40,000,000 for each of fiscal years 2023 through 2027” |
| Mental health and substance use disorder services on campus (42 U.S.C. § 290bb–36b) | “may award grants on a competitive basis to institutions of higher education to enhance services for students with mental health or substance use disorders that can lead to school failure, such as depression, substance use disorders, and suicide attempts, prevent mental and substance use disorders, reduce stigma, and improve the identification and treatment for students at risk, so that students will successfully complete their studies”; “Educating students, families, faculty, and staff to increase awareness of mental and substance use disorders”; “Supporting the training of students, faculty, and staff to respond effectively to students with mental and substance use disorders” | ORIGINATED FROM: Garrett Lee Smith Memorial Act, Pub. L. No. 108-355, § 3, 118 Stat. 1404, 1413-15 (2004) (“$5,000,000 for each fiscal year”) | “$7,000,000 for each of fiscal years 2023 to 2027” |
| Mental health awareness training grants (42 U.S.C. § 290bb–41(h)) | “nonprofit private entities to train teachers and other relevant school personnel to recognize symptoms of childhood and adolescent mental disorders, to refer family members to the appropriate mental health services if necessary, to train emergency services personnel, veterans, law enforcement, and other categories of individuals, as determined by the Secretary, to | ORIGINATED FROM: Children’s Health Act of 2000, Pub. L. No. 106-310, § 3213, 114 Stat. 1101, 1206-07 (2000) (“(b) MENTAL ILLNESS AWARENESS TRAINING GRANTS.— (1) IN GENERAL.—The Secretary shall award grants to States, political subdivisions of States, Indian tribes, tribal organizations, and nonprofit private entities to train teachers and other relevant school personnel to recognize symptoms of childhood and adolescent mental disorders, to refer family members to the appropriate support organizations”; “offer continuous and up-to-date information and awareness campaigns that target parents, family members, child care professionals, community care providers, and the general public and highlight the risk factors associated with youth suicide and the life-saving help and care available from early intervention and prevention services” | “$24,963,000 for each of fiscal years 2023 through 2027” |
| Bipartisan Safer Communities Act, Pub. L. No. 117-159, § 1313, 1340 (2022) | (“of the funds made available under this heading in this Act [$800,000,000, to remain available until September 30, 2025], the following amounts shall be for the following purposes in equal amounts for each of fiscal years 2022 through 2025 … $240,000,000 shall be for activities and services under Project AWARE [Advancing Wellness and Resilience in Education], of which no less than $28,000,000 shall be for activities described in section 7134 of Public Law 115–271” | | |
| Helping Families in Mental Health Crisis Reform Act of 2016 (division B of Public Law 114–255), § 9008, 130 Stat. at 1242 (“$5,988,000 for each of fiscal years 2018 through 2022”) | Restoring Hope for Mental Health and Well-Being Act of 2022 (title I of Public Law 117-328) § 1421 (“$9,000,000 for each of fiscal years 2023 through 2027”) | | |
| Helping Families in Mental Health Crisis Reform Act of 2016 (division B of Public Law 114–255), § 9008, 130 Stat. at 1243 (“$30,000,000 for each of fiscal years 2018 through 2022”) | Restoring Hope for Mental Health and Well-Being Act of 2022 (title I of Public Law 117-328) § 1422 (“$40,000,000 for each of fiscal years 2023 through 2027”) | | |
| Restoring Hope for Mental Health and Well-Being Act of 2022 (title I of Public Law 117-328) § 1423 (“$7,000,000 for each of fiscal years 2022 through 2023”) | Restoring Hope for Mental Health and Well-Being Act of 2022 (title I of Public Law 117-328) § 1424 (“$2,000,000 for each of fiscal years 2023 through 2027”) | | |</p>
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>identify and appropriately respond to persons with a mental illness&quot;; &quot;recognizing the signs and symptoms of mental illness&quot;</td>
<td>mental health services if necessary, to train emergency services personnel to identify and appropriately respond to persons with a mental illness, and to provide education to such teachers and personnel regarding resources that are available in the community for individuals with a mental illness…. (5) USE OF FUNDS.—A State, political subdivision of a State, Indian tribe, tribal organization, or nonprofit private entity receiving a grant under this subsection shall use funds from such grant to— (A) train teachers and other relevant school personnel to recognize symptoms of childhood and adolescent mental disorders and appropriately respond; (B) train emergency services personnel to identify and appropriately respond to persons with a mental illness; and (C) provide education to such teachers and personnel regarding resources that are available in the community for individuals with a mental illness…. (7) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this subsection, $25,000,000 for fiscal year 2001 and such sums as may be necessary for each of fiscal years 2002 through 2003.”) Helping Families in Mental Health Crisis Reform Act of 2016 (division B of Public Law 114–255), § 9010, 130 Stat. at 124 (“Mental health awareness training grants”; “inserting the following: ‘(A) Recognizing the signs and symptoms of mental illness’”; “$14,693,000 for each of fiscal years 2018 through 2022”) Bipartisan Safer Communities Act, Pub. L. No. 117-159, 136 Stat. 1313, 1340 (2022) (“of the funds made available under this heading in this Act [§800,000,000, to remain available until September 30, 2025], the following amounts shall be for the following purposes in equal amounts for each of fiscal years 2022 through 2025 … $120,000,000 shall be for Mental Health Awareness Training”) Restoring Hope for Mental Health and Well-Being Act of 2022 (title I of Public Law 117-328) § 1122 (“MENTAL HEALTH AWARENESS TRAINING GRANTS”; “$24,963,000 for each of fiscal years 2023 through 2027”) “$1,000,000 for the period of fiscal years 2023 through 2027”) “$120,000,000 shall be for Mental Health Awareness Training” “in equal amounts for each of fiscal years 2022 through 2025”</td>
</tr>
<tr>
<td>Mental and behavioral health outreach and education on college campuses (42 U.S.C. § 290ee–3)</td>
<td>“increase access to, and reduce the stigma associated with, mental health services”; “public education campaign that is designed to focus on mental and behavioral health on the campuses of institutions of higher education”; “improve the general understanding of mental health and mental disorders”; “encourage help-seeking behaviors relating to the promotion of mental health, prevention of mental disorders, and treatment of such disorders”; “make the connection between mental and behavioral health and academic success”; “assist the general public in identifying the early warning signs and reducing the stigma of mental illness”; “provides support for local efforts to reduce stigma by using the National Health Information Center as a primary point of contact for information, publications, and service program referrals” ORIGINATED FROM: Helping Families in Mental Health Crisis Reform Act of 2016 (division B of Public Law 114–255), § 9033, 130 Stat. at 1261 (“$1,000,000 for the period of fiscal years 2018 through 2022”) Restoring Hope for Mental Health and Well-Being Act of 2022 (title I of Public Law 117-328) § 1424 (continued from “2023 through 2027”) “$1,000,000 for the period of fiscal years 2018 through 2022”)</td>
</tr>
<tr>
<td>Grants to address the problems of persons who experience violence related stress (42 U.S.C. § 290hh-1)</td>
<td>“the development of knowledge with regard to evidence-based practices for identifying and treating mental, behavioral, and biological disorders of children and youth resulting from witnessing or experiencing a traumatic event.” ORIGINATED FROM: Children’s Health Act of 2000, Pub. L. No. 106-310, § 3102, 114 Stat. 1101, 1169-70 (2000) (“purpose of developing programs focusing on the behavioral and biological aspects of psychological trauma response and for developing knowledge with regard to evidence-based practices for treating psychiatric disorders of children and youth resulting from witnessing or experiencing a traumatic event”; “$50,000,000 for fiscal year 2001, and such sums as may be necessary for each of fiscal years 2002 and 2003.”) Helping Families in Mental Health Crisis Reform Act of 2016 (division B of Public Law 114–255), § 1004, 130 Stat. at 1261-65 (“the development of knowledge with “$50,000,000 for each of fiscal years 2019 through 2023.”)</td>
</tr>
</tbody>
</table>
regard to evidence-based practices for identifying and treating mental, behavioral, and biological disorders of children and youth resulting from witnessing or experiencing a traumatic event”; “$29,605,000 for each of fiscal years 2018 through 2022”)

9.3.1 Physician Health & Wellness (Issued 2016; Year Last Modified: 2017)

When physician health or wellness is compromised, so may the safety and effectiveness of the medical care provided. To preserve the quality of their performance, physicians have a responsibility to maintain their health and wellness, broadly construed as preventing or treating acute or chronic diseases, including mental illness, disabilities, and occupational stress.

To fulfill this responsibility individually, physicians should:

(a) **Maintain their own health and wellness** by:

   (i) following healthy lifestyle habits;
   (ii) ensuring that they have a personal physician whose objectivity is not compromised.

(b) **Take appropriate action when their health or wellness is compromised**, including:

   (i) engaging in honest assessment of their ability to continue practicing safely;
   (ii) taking measures to mitigate the problem;
   (iii) taking appropriate measures to protect patients, including measures to minimize the risk of transmitting infectious disease commensurate with the seriousness of the disease;
   (iv) seeking appropriate help as needed, including help in addressing substance abuse. Physicians should not practice if their ability to do so safely is impaired by use of a controlled substance, alcohol, other chemical agent or a health condition.

Collectively, **physicians have an obligation to ensure that colleagues are able to provide safe and effective care, which includes promoting health and wellness among physicians.**

Physicians and Physicians-in-Training as Examples for Their Patients to Promote Wellness and Healthy Lifestyles H-405.959 (Year Last Modified: 2019)

Our AMA will: (1) establish a program that recognizes physicians and physicians-in-training who model wellness and healthy lifestyles in their practice and communities or establish programs that contribute to the wellness of their patients and/or community; and (2) will aid in the development of a health and wellness component in conjunction with the Doctors Back to School Program.

Physician Health Programs H-405.961 (Year Last Modified: 2019)

1. Our AMA affirms the importance of physician health and the need for ongoing education of all physicians and medical students regarding physician health and wellness.
2. Our AMA encourages state medical societies to collaborate with the state medical boards to:
   (a) develop strategies to destigmatize physician burnout; and (b) encourage physicians to participate in the state’s physician health program without fear of loss of license or employment.
Inclusion of Medical Students and Residents in Medical Society Impaired Physician Programs
H-295.993 (Year Last Modified: 2018)

Our AMA: (1) recognizes the need for appropriate mechanisms to include medical students and resident physicians in the monitoring and advocacy services of state physician health programs and wellness and other programs to prevent impairment and burnout; and (2) encourages medical school administration and students to work together to develop creative ways to inform students concerning available student assistance programs and other related services.

8.1.3 Physician Competence, Self-Assessment and Self-Awareness (Issued: 2020; Year Last Modified 2020)

The expectation that physicians will provide competent care is central to medicine. It undergirds professional autonomy and the privilege of self-regulation granted by society. To this end, medical schools, residency and fellowship programs, specialty boards, and other health care organizations regularly assess physicians’ technical knowledge and skills.

However, as an ethical responsibility competence encompasses more than medical knowledge and skill. It requires physicians to understand that as a practical matter in the care of actual patients, competence is fluid and dependent on context. Each phase of a medical career, from medical school through retirement, carries its own implications for what a physician should know and be able to do to practice safely and to maintain effective relationships with patients and with colleagues. Physicians at all stages of their professional lives need to be able to recognize when they are and when they are not able to provide appropriate care for the patient in front of them or the patients in their practice as a whole.

To fulfill the ethical responsibility of competence, individual physicians and physicians in training should strive to:
(a) Cultivate continuous self-awareness and self-observation.
(b) Recognize that different points of transition in professional life can make different demands on competence.
(c) Take advantage of well-designed tools for self-assessment appropriate to their practice settings and patient populations.
(d) Seek feedback from peers and others.
(e) Be attentive to environmental and other factors that may compromise their ability to bring appropriate skills to the care of individual patients and act in the patient’s best interest.
(f) Maintain their own health, in collaboration with a personal physician, in keeping with ethics guidance on physician health and wellness.
(g) Intervene in a timely, appropriate, and compassionate manner when a colleague’s ability to practice safely is compromised by impairment, in keeping with ethics guidance on physician responsibilities to impaired colleagues.

Medicine as a profession should continue to refine mechanisms for assessing knowledge and skill and should develop meaningful opportunities for physicians and physicians in training to hone their ability to be self-reflective and attentive in the moment.
9.3.2 Physician Responsibilities to Impaired Colleagues (Issued 2016; Amended 2021)

Providing safe, high-quality care is fundamental to physicians’ fiduciary obligation to promote patient welfare. Yet a variety of physical and mental health conditions—including physical disability, medical illness, and substance use—can undermine physicians’ ability to fulfill that obligation. These conditions in turn can put patients at risk, compromise physicians’ relationships with patients, as well as colleagues, and undermine public trust in the profession.

While some conditions may render it impossible for a physician to provide care safely, with appropriate accommodations or treatment many can responsibly continue to practice, or resume practice once those needs have been met. In carrying out their responsibilities to colleagues, patients, and the public, physicians should strive to employ a process that distinguishes conditions that are permanently incompatible with the safe practice of medicine from those that are not and respond accordingly.

As individuals, physicians should:

(a) Maintain their own physical and mental health, strive for self-awareness, and promote recognition of and resources to address conditions that may cause impairment.
(b) Seek assistance as needed when continuing to practice is unsafe for patients, in keeping with ethics guidance on physician health and competence.
(c) Intervene with respect and compassion when a colleague is not able to practice safely. Such intervention should strive to ensure that the colleague is no longer endangering patients and that the individual receive appropriate evaluation and care to treat any impairing conditions.
(d) Protect the interests of patients by promoting appropriate interventions when a colleague continues to provide unsafe care despite efforts to dissuade them from practice.
(e) Seek assistance when intervening, in keeping with institutional policies, regulatory requirements, or applicable law.

Collectively, physicians should nurture a respectful, supportive professional culture by:

(f) Encouraging the development of practice environments that promote collegial mutual support in the interest of patient safety.
(g) Encouraging development of inclusive training standards that enable individuals with disabilities to enter the profession and have safe, successful careers.
(h) Eliminating stigma within the profession regarding illness and disability.
(i) Advocating for supportive services and accommodations to enable physicians who require assistance to provide safe, effective care.
(j) Advocating for respectful and supportive, evidence-based peer review policies and practices that will ensure patient safety and practice competency.
APPENDIX III. ACCREDITATION COUNCIL FOR GRADUATE MEDICAL EDUCATION (ACGME)
COMMON PROGRAM REQUIREMENTS


p.44: “Psychological, emotional, and physical well-being are critical in the development of the competent, caring, and resilient physician”

p.45: “Residents and faculty members are at risk for burnout and depression. Programs, in partnership with their Sponsoring Institutions, have the same responsibility to address well-being as other aspects of resident competence. Physicians and all members of the health care team share responsibility for the well-being of each other”

p.45: “accountability for physician well-being is crucial to physicians’ ability to deliver the safest, best possible care to patients.”

p.46: “VI.C.1.e) attention to resident and faculty member burnout, depression, and substance use disorders. The program, in partnership with its Sponsoring Institution, must educate faculty members and residents in identification of the symptoms of burnout, depression, and substance use disorders, including means to assist those who experience these conditions. Residents and faculty members must also be educated to recognize those symptoms in themselves and how to seek appropriate care”

p.46: “Programs and Sponsoring Institutions are encouraged to review materials to create systems for identification of burnout, depression, and substance use disorders”

p.46: “VI.C.1.e).(1) encourage residents and faculty members to alert the program director or other designated personnel or programs when they are concerned that another resident, fellow, or faculty member may be displaying signs of burnout, depression, a substance use disorder, suicidal ideation, or potential for violence”

p.46-47: “Individuals experiencing burnout, depression, a substance use disorder, and/or suicidal ideation are often reluctant to reach out for help due to the stigma associated with these conditions, and are concerned that seeking help may have a negative impact on their career. Recognizing that physicians are at increased risk in these areas, it is essential that residents and faculty members are able to report their concerns when another resident or faculty member displays signs of any of these conditions, so that the program director or other designated personnel, such as the department chair, may assess the situation and intervene as necessary to facilitate access to appropriate care. Residents and faculty members must know which personnel, in addition to the program director, have been designated with this responsibility; those personnel and the program director should be familiar with the institution’s impaired physician policy and any employee health, employee assistance, and/or wellness programs within the institution. In cases of physician impairment, the program director or designated personnel should follow the policies of their institution for reporting.”
COMMENTS OF THE KNOWING MACHINES RESEARCH PROJECT
Melodi Dincer,¹ Kate Crawford² & Jason Schultz³

to the
White House Office of Science and Technology Policy
RFI on Automated Worker Surveillance and Management
88 Fed Reg. 27,932
June 27, 2023

The Knowing Machines Research Project (Knowing Machines) submits these comments in response to White House Office of Science and Technology Policy’s (OSTP) May 3, 2023 Request for Information on Automated Worker Surveillance and Management (RFI).⁴ In alignment with its 2022 Blueprint for an AI Bill of Rights, OSTP is considering the “prevalence, impacts, and deployment” of worker surveillance technologies and how Federal agencies can help “ensure that these systems do not undermine workers’ rights or their safety.”⁵ The OSTP is considering a wide range of impacts on workers, including their “physical and mental health; privacy; dignity, and autonomy; and ability to exercise workplace rights.”⁶

We appreciate the opportunity to contribute to OSTP’s inquiry. Knowing Machines is an interdisciplinary research project tracing the histories, practices, and politics of how automated systems are trained to interpret the world from vast, nebulous datasets. Our research targets the assumptions underlying emerging machine-learning technologies with the hope that greater transparency will encourage meaningful interventions.⁷ We are a team of lawyers, computer scientists, science and technology studies (STS) professors, artists, and data scientists who have

¹ Legal Research Fellow, The Knowing Machines Research Project; Supervising Attorney, NYU’s Technology Law & Policy Clinic, and Fellow, Engelberg Center on Innovation Law & Policy, NYU School of Law.
² Lead Principal Investigator, The Knowing Machines Research Project; Research Professor of Communication and STS, USC Annenberg School for Communication and Journalism; Senior Principal Researcher, Microsoft Research Lab (NYC).
³ Co-Principal Investigator, The Knowing Machines Research Project; Professor of Clinical Law, Director of NYU’s Technology Law & Policy Clinic, and Co-Director of the Engelberg Center on Innovation Law & Policy, NYU School of Law.
⁵ Id. at 27,934.
⁶ Id.
⁷ For more information, see https://knowingmachines.org.
published extensively on the techniques and harms of automated surveillance technologies, including in the workplace—whether that be the factory floor, warehouse, office, or the home.⁸

Knowing Machines urges OSTP to translate workers’ expectations of privacy in their data into guidance for employers on when and what types of data they can collect. As worker data fuels automated surveillance technologies by serving as training data for machine-learning models, we encourage OSTP to set a high bar for employers who exploit worker data to inform employment decision and undermine workers’ autonomy. Specifically, we propose OSTP collaborate with other federal agencies to set baseline protections over worker data that align with the limits on health data for healthcare providers and on consumer financial data for financial institutions respectively. At a minimum, we hope OSTP will adopt clear policies protecting worker data relating to union organizing communications and activities.

1. Automated Worker Surveillance and Management Systems Depend on Massive Amounts of Worker Data

The pandemic and its aftermath have intensified existing rifts over worker autonomy and control in the U.S.⁹ Especially as young adults enter a workforce shaped by decades-long wage stagnation, anemic unionization, and regular waves of mass layoffs, they are proving immune to the promises of “workism”—the belief that “work is not only necessary to economic production, but also the centerpiece of one’s identity and life’s purpose.”¹⁰ Attention-grabbing buzzwords like “the Great Resignation”, “quiet quitting”, and the “anti-work movement” attempt to capture a

---


⁹ See Limitless Worker Surveillance, supra note 8, at 111–13 (describing the changing nature of work in the U.S., including pre-pandemic increases in remote workers and freelance workers).

broader sense of turmoil in our relationship to work, boundaries, and living a meaningful life both in and beyond our jobs.\textsuperscript{11}

Yet workism persists, with around 40\% of workers seeing their jobs as central to their overall identities regardless of gender, race, ethnicity, or age.\textsuperscript{12} While certain groups of workers—educated young men, high-earners, and recovering workaholics—are spending less time working than pre-pandemic,\textsuperscript{13} employers continue to project their “productivity paranoia” onto workers of all stripes.\textsuperscript{14} This has led to a sharp increase in surveillance technologies permeating the average workday. Searches for employee monitoring software increased by 75\% in March 2020 compared with the 2019 monthly average, and now around 80\% of employers use monitoring software to track employee performance and online activity.\textsuperscript{15}

Today, technology is a critical factor in both what we do for work and how we do it. But while employers have been rapidly adopting new methods of AI-driven automated worker surveillance,\textsuperscript{16} this phenomenon is a continuation of much older labor practices established in the late nineteenth and early twentieth centuries.\textsuperscript{17} As one of us has previously noted, “[w]e are witnessing new refrains on an old theme.”\textsuperscript{18} The atomized, tedious work of early factories

\textsuperscript{16} In this Response, we focus on machine learning-based technologies of worker surveillance. We use the term “AI”, aware of its misleading anthropomorphism, to refer to technical systems that rely on machine learning models trained on datasets to extract patterns and use those patterns to predict outcomes in new contexts. See generally Sarah Clston, \textit{A Critical Field Guide for Working with Machine Learning Datasets} (2023), https://knowingmachines.org/critical-field-guide.
\textsuperscript{17} See ATLAS of AI, supra note 8, at 59 (“The encroachment of AI into the workplace should properly be understood as a return to older practices of industrial labor exploitation that were well established in the 1890s and the early twentieth century.”); Saima Akhtar, \textit{Employers' New Tools To Surveil and Monitor Workers Are Historically Rooted}, Wash. Post (May 6, 2021), https://www.washingtonpost.com/outlook/2021/05/06/employers-new-tools-surveil-monitor-workers-are-historically-rooted/ (“The history of worker surveillance shows that today’s cutting-edge time-tracking technologies are just new iterations of an old industrial technique—only now, these technologies are more discreet and pervasive.”). For a robust historical analysis of worker surveillance in the U.S., see Irem Arı unwa, \textit{The Quantified Worker: Law and Technology in the Modern Workplace} 179–87 (2023).
\textsuperscript{18} ATLAS of AI, supra note 8, at 29.
required managers to maintain efficient and disciplined workers. This necessitated new systems of observation and control for managers that drew from earlier systems, including the 1780s’ inspection house that placed all of a factory’s workers within constant sight of their supervisors, and the central role of overseers for slave owners in the plantation colonies of the Americas. This historic oversight role has been “primarily deputized to surveillance technologies” today. But what these technologies enable is a more granular and invasive degree of worker surveillance than historical human managers could ever dream of.

There are several types of automated worker surveillance. Much of it is deployed to placate the employer that workers are really working. This includes activity monitoring, or surveilling how workers spend their time through tools that “track idle time, record keystrokes, or even periodically screenshot an employee’s computer.” But there are also several types of surveillance that go beyond monitoring productivity to uncover workers’ personal behaviors and characteristics. So-called “bossware” programs that monitor and collect data from workers’ emails, telephones, and online activities can be used to gauge productivity, but that data can also reveal personal behaviors and characteristics with no connection to one’s work. Other examples include location tracking, video camera surveillance, measuring workers’ use of different applications on digital devices, and even biometric surveillance tools that use facial recognition to ensure that workers remain in front of their computer screens during business hours. Behavioral surveillance tools not only measure productivity and compliance with company policies, but some also attempt to predict when workers might be likely to quit. And tools like emotion recognition analysis are used to gauge a job candidate’s “fit” with the

19 See id. at 60–61.
20 Id. at 61–63.
21 Id. at 62.
22 Akhtar, supra note 17 (“Although the surveillance and punishment of ‘wasted time’ on the factory floor has remained fairly consistent over the past century, the way workers’ time gets tracked and recorded has become more invasive due to advancements in technology.”).
23 A full survey is outside of the scope of this Response but can be found in various publications. See, e.g., Ajunwa, supra note 17, at 187–92 (2023) (providing an overview of modern worker surveillance); Limitless Worker Surveillance, supra note 8, at 108–113 (gathering similar examples).
24 Ajunwa, supra note 17, at 189.
26 See Ajunwa, supra note 17, at 190–91.
27 Id. at 191.
prospective employer, based on pseudoscientific conclusions about the ways we express emotions through facial gestures alone.\textsuperscript{28} Sometimes, data collected from costumers—like their traffic patterns and other interactions with products and employees—lead to indirect worker surveillance, informing employers how many workers to schedule and where.\textsuperscript{29}

These technologies inform the field of “people analytics” built on the vast digital data generated mostly passively as workers perform their daily activities.\textsuperscript{30} Its central premise is that as much data must be collected as possible, so that these data can provide accurate insights into persistent managerial questions, including who to hire or promote, who is likely to leave, who has been working collaboratively despite working remotely, and whether workers feel fulfilled professionally.\textsuperscript{31} The algorithms that interpret these data are increasingly used to inform employment decisions, whether or not workers are aware of the surveillance.\textsuperscript{32}

People analytics beget an intimately quantified modern worker.\textsuperscript{33} Whereas Taylorist theories of management focused on mastering a single task along the assembly line and maximizing production efficiency, people analytics has shifted focus onto the individual worker as a cite of self-mastery to save the employer time and money.\textsuperscript{34} Surveillance technologies allow employers to be omnipresent in each of their workers’ lives without physically being anywhere near them, enabling uninterrupted monitoring of a person’s communications, movements, and activities even outside of work.\textsuperscript{35} Employers have converted their workers into “captive audiences for data extraction,” using these technologies to indiscriminately capture and transfer worker data that is


\textsuperscript{29} Ajunwa, supra note 17, at 174.

\textsuperscript{30} See Jeffrey T. Polzer, The Rise of People Analytics and the Future of Organizational Research, 42 ORGANIZATIONAL BEHAV. 1 (2023), https://www.bbe.edu/rie/Publication%20Files/1-s2.0-S0191308523000011-main_0230d385-13af-4a01-9b68-c6b07be05ce2.pdf.

\textsuperscript{31} Id. at 1.

\textsuperscript{32} Id. at 3 (“Workers are being quantified as never before as the ongoing digital revolution converts every action and interaction into a trail of data. These data can be fed into algorithms, which can then produce predictions, categorizations, and suggestions to change behavior.”). See also Alex Christian, The Employee Surveillance that Fuels Worker Distrust, BBC (June 27, 2022), https://www.bbc.com/worklife/article/20220621-the-employee-surveillance-that-fuels-worker-distrust (“Often, this [bossware] technology runs undetected, meaning workers can be unaware that their boss is effectively spying on them.”).

\textsuperscript{33} See generally Ajunwa, supra note 17.

\textsuperscript{34} Limitless Worker Surveillance, supra note 8, at 137.

\textsuperscript{35} Id. at 138; see also Ajunwa, supra note 17, at 175 (“Surveillance technologies are what has enabled management to become less visible, yet more powerful.”).
often personal and sensitive. For our colleague and worker surveillance expert Ifeoma Ajunwa, this data is “captured capital” as it “is siphoned from workers both knowingly and unknowingly as part of the employment bargain.” Workers have no uniform privacy protections to this data, and they largely lack any bargaining power over how employers exploit their data.

There is a direct link between the exploitation of worker data and automated worker surveillance. Put simply, “[d]ata obtained through employee surveillance fuels AI.” As worker data becomes more legible and sortable into distinct categories, it can be used to train machine-learning models that undergird AI technologies used to interpret worker behavior. This creates a dangerous cycle: workers use technologies that produce data, that data is compiled into vast datasets, those datasets are used to train models, those models influence algorithms to find certain associations in the data, and then those algorithms power automated surveillance tools used by employers to decide whether workers are being sufficiently productive, loyal, and compliant. Pairing the “voracious maw of data collection” with the “inexplicability of decisions made” from automated systems leads to workers feeling “trapped in a matrix of computer-controlled reality from which there is no escape.”

There is growing concern about the misuse of data to train machine-learning models powering automated surveillance technologies, and worker data should be no exception. In its consideration of automated worker surveillance systems, OSTP must be mindful of the enclosure of worker data that enables the development of these systems in the first place. The lack of clear privacy protections for worker data provides OSTP a unique opportunity to guide employers on when and what types of worker data they can collect, store, use, and sell. OSTP must act now to

---

36 AJUNWA, supra note 17, at 178.
37 Id. at 177.
38 Limitless Worker Surveillance, supra note 8, at 113–28 (analyzing extant legal protections and their weaknesses).
39 See ATLAS OF AI, supra note 8, at 58 (“The terms of AI in the workplace] are based on a significant power asymmetry—is there ever a choice not to collaborate with algorithmic systems? When a company introduces a new AI platform, workers are rarely allowed to opt out.”); Kate Crawford, Amazon’s Union Vote Could Be a Harbinger for the Future of Work, WASH. POST (Apr. 10, 2021) (“Artificial Intelligence systems are increasingly used to track, assess, and rank workers—often without their knowledge. This, in turn, acts as a force multiplier for the asymmetries of power between bosses and employees.”); Pauline T. Kim & Matthew T. Bodie, Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy, 35 ABA J. LABOR & EMP. L. 289, 292 (2021), https://www.americanbar.org/content/dam/aba/publications/aba_journal_of_labor_employment_law/v35/n02/artificial-intelligence.pdf (“Employees report a feeling of powerlessness when AI is given significant power over their jobs, as they lose the ability to interact with their ‘supervisor’ in a meaningful way.”).
40 Kim & Bodie, supra note 39, at 301.
41 Id. at 292.
counterbalance employers’ insatiable thirst for more comprehensive and invasive worker data to fuel people analytics solutions, bringing autonomy over worker data explicitly into the conversation.

II. OSTP Should Adopt Baseline Worker Data Privacy Guidance to Deter Unchecked Worker Surveillance by Employers

In its Blueprint for an AI Bill of Rights, OSTP recognized that individuals and their communities “should be free from unchecked surveillance; surveillance technologies should be subject to heightened oversight.”\textsuperscript{43} Responding to Question 5. of the RFI, Knowing Machines encourages OSTP to develop guidance for employers who currently deploy automated worker surveillance systems or are considering doing so.\textsuperscript{44} We are mindful that often specific statutes and regulations governing security, access, and notice and consent regimes “provide insufficient guidance for decisions about the reuse and repurposing of information when companies can manipulate huge amounts of data” collected through worker surveillance.\textsuperscript{45} Instead, we agree that “broader principles have to be developed that can guide privacy decisions consistently in a variety of contexts,” and those broader principles should draw from workers’ own expectations about their data “as a touchstone for developing [employers’] privacy practices, including the [employer’s] definition of privacy.”\textsuperscript{46} Beyond simply punishing bad behavior, federal agencies beginning with OSTP must encourage employer responsibility for protecting worker privacy.\textsuperscript{47}

Because automated worker surveillance technologies require vast amounts of worker data for training purposes, employers are currently incentivized to collect worker data with abandon. OSTP should consider adopting guidance that proposes internal guardrails for employers over when and what types of worker data they are able to collect and process. To this end, we suggest OSTP help disincentive limitless worker surveillance by encouraging employers to treat worker...
data with the same level of care that healthcare providers treat health data and financial institutions treat consumer financial data. This guidance should be informed first and foremost by workers' own expectations of privacy over their communications, locations, behaviors, and other forms of personal data, especially where employers cannot show that these data and work performance are connected or such connections are attenuated at best.

Furthermore, we encourage OSTP to explore numerous worker data protections that will impact the viability of automated surveillance technologies driven by AI today. First, OSTP should work with other agencies to develop data privacy requirements in vendor agreements for automated surveillance products, including strict data minimization procedures and use limitation requirements to ensure that only the necessary amount of data is collected for a specific employment use (ideally limited to human resources and diversity initiatives), and data collected in one context is not later applied in employment decisions in other contexts. For companies that collect worker data into databases that could be used to train automated technologies, OSTP can incentive greater clarity around database access and licensing by requiring employers to appoint dataset stewards who can decide and document how datasets may be used, derived from, and distributed outside of the employer.

Additionally, OSTP can work with organized and organizing workers fighting back against automated worker surveillance to protect them from employer interference and retaliation. In line with recent decision by the National Labor Relations Board against Amazon's anti-union surveillance efforts, OSTP can adopt clear policies prohibiting the collection of worker data

---


50 See Ajuanwa, supra note 17, at 202 (discussing how, when state law does not specifically prohibit worker surveillance, courts weigh an employer's need to conduct surveillance against the employee's reasonable expectation of privacy); Ifeoma Ajuanwa, Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, 63 ST. LOUIS U. L.J. 21, 49 (2018), https://scholarship.law.shul.edu/jl/vol63/iss1/4/ (“While a reasonable expectation of privacy is well defined for Fourth Amendment cases, it is not as defined within the employment context, and some scholars have argued that workplaces operate as ‘private governments’ with employers exercising near dictatorial power over what privacy rights may be granted to workers.”).

51 See Feng, Mathur & Narayan, supra note 42, at 9–10 (describing how dataset creators should best steward datasets to minimize downstream misuses of the underlying data).
related to organizing and union participation. By protecting workers from the weaponization of their data to thwart organizing efforts, OSTP will enable workers to collectively bargain with their employers about the specific, context-dependent limitations they seek over their own workplace surveillance and their employers’ access to their personal data.

III. Conclusion

Knowing Machines supports OSTP’s critical inquiry into the massive reach of automated worker surveillance technologies and their negative impacts on workers’ lives. OSTP should develop guidance on baseline privacy protections that mediate the inherent power differential between employers and workers over control of their data. We encourage OSTP to emphasize the centrality of worker data to automated surveillance technologies powered by AI, as worker data informs the training of models that then influence algorithmic decision-making in opaque and unjust ways. If OSTP has any further questions, please reach out to Legal Research Fellow Melodi Dincer at [redacted] or Co-Principal Investigator Jason Schultz at [redacted].

Respectfully Submitted,

(b) (6)

Melodi Dincer
Legal Research Fellow
Knowing Machines Research Project


Kate Crawford
Lead Principal Investigator
Knowing Machines Research Project

Jason Schultz
Co-Principal Investigator
Knowing Machines Research Project
Response to OSTP request for comments on Automated Tools Being Used to Surveil, Monitor, and Manage Workers

June 15, 2023

For additional information about this response, please contact:

Ezra Asumey
Human Computer Interaction Institute
Carnegie Mellon University

About Our Research Team

Rooted in the strong belief that today’s socio-technical problems require a uniquely interdisciplinary approach, our research team consists of experts in the fields of human-computer interaction, data privacy and policy. Our team has been awarded multiple NSF grants to research the effects of automation technologies on the future of work and personal data privacy towards the design of solutions that maximize opportunities and positive outcomes for workers. A significant part of our mission goes beyond research; and involves cultivating synergistic relationships between worker advocacy groups, academia, government agencies, and businesses. We view such multi-institutional collaborations as necessary for the establishment of regulatory frameworks that protect the rights, well-being and dignity of workers, while also harnessing the benefits of the technologies that drive economic progress. People are the heart of our work, our goal is to leverage these strategic partnerships to place the well-being of workers at the center of technological advancements.

We’d like to thank the OSTP for the opportunity to comment on Automated Tools Being Used to Surveil, Monitor, and Manage Workers.

Introduction and Overarching Recommendations

Present-day operational realities demonstrate a heightened reliance on biometric technologies in the workplace. The US workplace biometrics industry is projected to grow from its current size of $4.9 billion to $11.4 billion by the end of the decade.¹ While originally conceived of as an approach for verifying the identities of individuals for accessing buildings or electronic devices, recent trends suggest that AI-augmented biometrics will increasingly be used

¹ https://www.imarcgroup.com/united-states-biometrics-market
for employee performance monitoring. We argue that as a result, the necessity for bold early-stage regulatory interventions has become apparent.

Biometrics refers to the measurement and statistical analysis of an individual’s physical and behavioral characteristics, such as facial expressions, brainwaves, or keystroke patterns. These data can be used to make inferences about various aspects of a worker’s status such as, mood, alertness and productivity respectively. While in some settings these tools have proven beneficial in enhancing worker safety, they bring into sharp focus concerns surrounding privacy, consent, transparency, and potential misuse.

We are witnessing the development of a high-stakes technology landscape where the implementation of biometric monitoring in the workplace can pose threats to employees' privacy and personal well-being unless properly managed.

Response to Question 5A: What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers' rights?

We outline five strategies for maintaining a balance between harnessing the benefits of biometric monitoring technologies and protecting employees' rights and privacy:

1. **Require employer transparency on the use of biometrics across the employment lifecycle.**
2. **Develop a national database tracking employer usage of worker biometric data.**
3. **Place limitations on biometric data sharing between companies.**
4. **Require employers to adjust company operations in response to harmful working conditions surfaced through biometric data collection.**
5. **Regulate vendors of biometric performance monitoring technologies.**

Mandate Employer Transparency Across the Employment Lifecycle

Employer transparency on the use of biometric performance monitoring technologies is an essential protection for workers. This involves informing any potential and existing employees verbally and in writing about the collection, use, storage, and potential sharing of their biometric data during the tenure of their employment. All employees subject to biometric performance monitoring should be thoroughly educated about their rights with respect to consenting to such procedures and the possibility of opting out. Furthermore, employees should

---

4 https://publications.jrc.ec.europa.eu/repository/handle/JRC125716
be notified about changes in company practices surrounding biometric data capture, use, and storage. Finally, employers should be required to completely remove employees' biometric data from their records at the end of their employment.

The adoption of such measures will be critical for workers to make informed decisions when determining whether the conditions of employment are in alignment with their values, personal comfort levels, and privacy expectations.

**Tracking the Use of Biometric Data**

We strongly advocate for the establishment of a national database that tracks companies’ usage of biometric data to make decisions affecting the status of workers, including but not limited to, terminations, suspensions, and promotions. Such a system would provide data related to the type of biometric information used, the justification for its use, and subsequent outcomes. Regular audits of this database through a regulatory commission acting on behalf of the Department of Labor will aid the identification and rectification of any potential biases, ensuring the objective and fair use of biometrics in compliance with title 29 of the Code of Federal Regulations.\(^5\)

**Limitations on Biometric Data Sharing Across Companies**

Employee privacy and rights should be safeguarded by imposing restrictions on the sharing of biometric data among employers. Without such measures, inaccurate and unjustified inferences drawn from an employee's biometric data could unfairly hamper their future employment opportunities. Clear policies and legal frameworks need to be established that delineate the conditions under which employee data can be accessed and the purposes for which it can be used. Consent from the employee must be a prerequisite for any data sharing, and any infractions of these rules should incur high penalties. (e.g., require businesses to recompense harmed employees in an amount commensurate to missed earnings.)

**Require Companies to Address Harmful Working Conditions Surfaced through Biometric Data Collection**

Business monitoring their employees’ biometric data should be compelled to report and address harms to workers surfaced through the collection of biometric data. Should a firm discover that the conditions of work result in high rates of worker injury and fatigue, they must take meaningful actions to reduce the harm. This might be achieved, for example by modifying working conditions, or through additional workforce training. Targeted OSHA inspections should come as a consequence for firms unable to keep work-related harm below a set threshold.

---

\(^5\) [https://www.ecfr.gov/current/title-29](https://www.ecfr.gov/current/title-29)
Vendor Accountability

The role of vendors in developing and supplying these technologies, therefore, carries significant implications. Currently, the United States stands as a key global player in the design and distribution of workplace monitoring technologies, with advanced product offerings.\(^6\) We also recognize some glaring issues, such as vendor accountability, standardization, and regulatory compliance, which can affect the just and equitable deployment of these technologies.

We argue that NIST should set standards to ensure the quality and robustness of datasets used in biometric technologies, given their significant implications for accuracy and fairness. These standards should address data diversity and representativeness and provide guidelines for handling missing or inaccurate data. Moreover, the complexity of inferences drawn from predictive biometric technologies should be considered, and the reasoning for these inferences should be transparent, comprehensible, and data justified.

Vendors should bear responsibility for the secure storage, handling, and transmission of biometric data. This should also extend to the disclosure of any data breaches and third-party sharing and usage of data for purposes not explicitly approved by the client or the users. In cases where vendors fail to comply with these standards, penalties should be imposed as a deterrent.

Vendors must adhere to strict industry standards for data quality and robustness and they should be expected to demonstrate their compliance with these standards before their products can be deployed. Finally, vendors must be required to provide comprehensive documentation detailing how their technology operates, the data it collects, what inferences it makes, how accurate it is, and how it will use and store this data. Federal, regulatory oversight is needed to monitor and enforce these compliance standards.

\(^6\) [https://www.imarcgroup.com/biometrics-manufacturing-companies](https://www.imarcgroup.com/biometrics-manufacturing-companies)
June 18th 2023
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504
Attn: Dr. Alan Mislove

Re: Request for Information: Automated Worker Surveillance and Management,
Document ID OSTP-TECH-2023-0004-0001

To Whom It May Concern:

We write to offer public comment on the request for information published on May 2, 2023 (Document 2023-09353). Coworker welcomes this public consultation by the White House Office of Science and Technology Policy (OSTP) on automated worker surveillance and management technologies. Coworker is a laboratory for workers to experiment with power-building strategies and win meaningful changes in the 21st-century economy.

For the past four years, we have been conducting participatory field and market research and analysis on how data-mining techniques innovated in the consumer realm had moved into the workplace¹ and job markets. The past two years, we have been investigating and documenting the increasing number of tech products and tech companies intersecting with every step of the labor process — hiring/recruitment, workplace safety and productivity, benefit provision, workforce development, et al. Dubbing this tech ecosystem as “Little Tech”, we launched a public database² to bring attention to the rapidly growing and expansive unregulated marketplace of tech products increasingly collecting, aggregating, and analyzing sensitive data from workers. We have also been working alongside workers to understand how algorithmic payroll systems impact workers’ wages, through our work with Shipt workers (see: Some Shipt workers report seeing lower pay under new effort-based model.)

² “Bossware and Employment Tech Database.”
The impact of algorithmic management tools and surveillance on workers has to be understood within the broader labor and market realities. Specifically, the proliferation of algorithmic workforce management tools have to be understood within a context of decreasing productivity gains, workers’ weakening ability to organize and collectively bargain, ongoing fissuring of the workplace and job markets, and past regulatory precedent from the DOJ and FTC specifically calling out the role of HR in maintaining a competitive market for their employment, not only in hiring and recruitment but in any harmful conduct that stifles competition and can lead to decreased wages, less attractive benefits, or even lost job opportunities.

We have found that while the suite of products in this employment tech marketplace seek to fulfill a variety of HR business purposes, these products pose a variety of risks and harms for workers that extend beyond privacy, and go into economic well-being, health, including mental health. We are also seeing that with increased focus on intrusive algorithmic management and workplace surveillance tools, that vendors are beginning to rebrand in an attempt to fly under the radar. One particular vendor that has done this is Activtrak. Activtrak is a well-known highly-intrusive productivity monitoring vendor that’s been around for a while. They were among the first doing keyboard logging tracking and now have a more sophisticated set of tools. In the past two years they have become more vocal about taking privacy seriously and it would be good to check what they say. They also have a Productivity Lab with tech experts that are trying to understand workplace trends and provide tips with employers that would be good to engage with. Therefore, it is important to stay hyper vigilant of this rapidly changing field of employment technologies.

In order to assist OSTP’s analysis of public and private uses of automated worker surveillance and management tools, below is an overview of the current and anticipated uses of these technologies in the workplace and job markets.

(1) Increased diversification and sophistication of HR and workforce management tools:

Through our research and conversations with workers we have been tracking the evolution of HR-focused and workforce management tools over the past five years. We have found that during this time the suite of tools has expanded to a wide variety of new vendors that now also include employer listening tools, identity verification and background screening tools and labor data brokers and intelligence vendors.
Additionally, the evolving suite of tools and solutions are being aided through increased tech capabilities such as the use of facial recognition and various forms of AI such as emotionAI, conversational AI, computer or video vision and AI, wearable devices, etc.

- **Employee listening tool, Prodoscore**: This vendor is mostly a workplace productivity monitoring tool, but they have a Social Network feature that allows employers to "visualize how people are connected, how they communicate, and what influence they have on each other" which could be problematic for detecting organizing in the workplace. More here: [https://www.prodoscore.com/social-network/](https://www.prodoscore.com/social-network/).

- **Employee listening tool, Infeedo.AI**: they call their solutions "continuous listening at scale". They report to be growing rapidly in the past two years, although it's hard to see the list of their customers.

- **Employee listening tool, Oracle**: has a new employee listening tool and it's not very transparent on what data it's collecting. More investigation and research is needed. More on this article: “[Oracle's new platform latest sign of growth in employee listening](https://www.prodoscore.com/social-network/)”.

- **Workplace productivity tool that utilizes facial recognition, Clever Control**: Highly intrusive workplace productivity monitoring vendor that has been around a long time. Also utilizes facial recognition as [one of their customer stories shows](https://www.prodoscore.com/social-network/). Not very transparent about which employers use them, but they seem to cater to the public and private sector.

- **Employee listening tool, Aware**: Collects sentiment and productivity data on workers and frames it as empathetic employee listening. Used in a lot of Fortune 100 and Fortune 200 companies, but not very transparent with who the customers are.
(2) Widespread collection of workers’ data inside and out the workplace:

While earlier products collected passive data, such as time logging, keystrokes, websites visited, etc, algorithmic management tools are now collecting an increasing number of data points on workers that include things such as tracking of physical movements, as well as facial and audio data and sensitive physiological biometrics data such as gestures, sentiment/mood, stress levels, cognitive functioning, etc, health such as workers’ medical/health info (i.e. body temperature, respiratory rate, and heart rate³).

Vendors in this category include:

- **Invisible AI**: uses cameras and algorithms to track workers’ body movements as they work through assembly processes.

- **VoxelAI**: used in retail, warehouses, and manufacturing. It is a highly intrusive product that utilizes "computer vision and AI to enable security cameras to automatically identify hazards and high-risk activities in real-time, keeping people safe."

- **Wearable tech, Modjoul**: Founded in 2016 and based in Greenville, South Carolina, Modjoul is developing wearable safety technology that enables real-time, personalized alerts and recommendations aimed at reducing injuries, most notably musculoskeletal issues.

We are also finding that some vendors are scraping public data on workers (social media information, press releases, google search results, etc) and packaging them up as labor intelligence data that can be bought and integrated into workforce management tools.

Vendors acquiring and integrating workers’ public data into workforce management tools include:

- **Physiological biometrics data collection**, WorkHuman: this vendor calls itself the world’s fastest-growing integrated Social Recognition® and Continuous Performance Management platform to help build a positive workplace culture. However, their tool collects data from workers to predict worker motivations, behaviors, and sentiment. You can read about their MoodTracker and other analytics here: [https://www.workhuman.com/workhuman-iq/](https://www.workhuman.com/workhuman-iq/).

³ See Scorecard by Fight for the Future highlighting which top retailers are employing facial recognition technologies in the workplace: [Ban Facial Recognition In Stores](https://www.fightforthefuture.org/ban-facial-recognition-in-stores).
• **Employment data broker, Equifax/Appriss Insights** (acquired by Equifax): Prior to its acquisition in 2021, Appriss Insights administered the nation’s most comprehensive source of person-based incarceration, justice, and risk intelligence data. After its acquisition by Equifax (press statement here), it was integrated into the Equifax Total Verify platform which among different solutions, includes a workforce management solution for “Workplace Safety” screening and employment verification.

• **Employment data broker, CLARO**: Claro describes itself as a “global labor market intelligence platform” collecting and aggregating billions of data points to benchmark worker attrition risk and worker engagement. They seem to be affiliated with the Human Data Interaction Project at MIT. But other than that, it is unclear their process for aggregating employment data from public records and how that data is modeled into predictive tools for employers.

Finally, the switch to hybrid and remote work has increased the demand for management tools that can provide employers with visibility into employee activities discreetly and in the ability to surveil remote or hybrid workers after working hours. Two particularly, problematic vendors we want to identify are:

• **Teramind**: This is one of the more intrusive algorithmic workplace management vendors we’ve seen that also collect biometric data as part of their monitoring and is used to monitor remote work.

• **Teleperformance TP Observer**: provide an AI-enabled webcam that can be installed in remote workers’ computers that recognizes their face, tags their location, and scans for “breaches” of rules at random points during a shift. Such breaches include an “unknown person” detected at the desk via the facial recognition software, “missing from desk,” “detecting an idle user,” and “unauthorized mobile phone usage”. Other products such as Teramind, collect audio recordings from workers (without their knowledge) among other employee activity data points in order to support workplace investigations.
Widespread data collection is being used to increase employers’ intelligence capabilities to conduct (1) risk modeling and predictive analytics, (2) disaggregate job duties and assign economic value, and (3) design AI systems to work alongside workers to make them more productive and “effective”:

These black box predictive and risk modeling systems are being used to measure everything from workers’ productivity to predict workers’ mood and sentiments, their cultural fit, and specific targeted analysis to identify workers at risk of unionizing or going “rogue.” We have also found that these black boxes can be customized by employers to target whichever problematic behaviors they are most concerned about (e.g. tardiness, productivity, workplace organizing, workplace violence, etc) and there is not a lot of transparency on what problematic behaviors they can target, predict, and rank worker for and how this analysis is made.

Vendors that process workers’ data through black box risk modeling and predictive analytics are:

- **Risk Modeling/Insider Threat Detection: Verensics**: Their Human Resource Solution includes the use of a “Visual Risk Index” to help employers weed out potential new employees in their “areas of concern” at the screening stage. Their proprietary algorithm appears to create a unique profile for each candidate and multiple data points are analyzed in real-time. It is unclear whether public records data is being used in the modeling.

- **Risk Modeling/Insider Threat Detection, Forcepoint Behavioral Analytics (acquired by Francisco Partners)**: They have an Insider Risk Detection tool that collects a lot of workers’ behavioral data. You can find a data fact sheet on this solution on their site: https://www.forcepoint.com/product/fit.

- **Risk Modeling/Insider Threat Detection: Veriato Cerebral (acquired by Awareness Technologies)**: Veriato Cerebral is a user behavior analytics and insider threat management solution that’s powered by machine learning algorithms. It monitors employee chats, emails, web surfing, and file transfers and uses other data to develop a Risk Score profile for each worker that is updated daily. We are not sure what other data may be integrated into their Risk Profile of workers. More here on their proprietary Risk Profile: https://www.veriato.com/products/veriato-cerebral-insider-threat-detection-software.

- **Risk Modeling/Insider Threat Detection, Forcepoint Behavioral Analytics**: This vendor has been around for over 10 years and is an established player in
the field of employment risk detection tools. They have an Insider Risk Detection tool that collects a lot of workers' behavioral data. You can find a data fact sheet on this solution on their site: https://www.forcepoint.com/product/fit.

- **Fraud detection: Pondera Solutions:** It was acquired by Thomas Reuters in 2020 and is now called Fraud Detect solution for Thomas Reuters. This new solution under Thomas Reuters is now used to detect unemployment scams. More information is needed regarding its machine learning modeling and collecting of data.

With increased focus on generative AI, and the ability for these tools to fragment workers' tasks, understand time spent per task, and economic value to employers, that this may lead to wage instability for workers who may find that employers may begin disaggregating job tasks and assign arbitrary cost value to particular job duties without a workers’ knowledge or awareness. So, this is a trend we are watching closely.

Finally, we are seeing workforce management tools that teach workers to work alongside AI systems in order to teach them to be more productive and “effective” at their job. Two particular vendors we’ve been monitoring are used in call center work are:

- **Chorus:** company claims to be "**backed by 14 technology patents that leverage proprietary machine-learning, Chorus is the fastest growing Conversation Intelligence product in existence**".

- **Cogito:** claims to be "**used by 5 of the Fortune 25 brands across diverse industries including healthcare payers; property, casualty, and life insurers; telecom and cable providers.**" Utilizes what it calls an Emotion AI and Conversational AI to support Call Center workers.

- **Biointellisense:** this vendor is being used in the home health aide industry as we heard from the worker last week. Its tag line is: "**Patient-centered, data driven care built for scale.**" It’s unclear about how it includes the voices and concerns of home health care providers in the development of its data-driven platform.
Now that we have outlined the marketplace of algorithmic management products, below we discuss key areas where OSTP’s leadership would be a much-needed intervention in helping to provide better protections and redress for workers.

- **Engage vendors in order to increase greater transparency over data collection and processing:** The marketplace includes established corporate actors such as Experian, Oracle, and long standing workplace productivity vendors such as Activtrak, Teramind, etc., and a variety of emerging AI startups. As a result, there is competition and gatekeeping taking place between established and emerging vendors in this space, which contributes to the lack of transparency. OSTP is well-placed to convene this industry in order to better understand the functionalities of the products and the potential risks and harms to workers. This effort should be done jointly with other key labor regulatory agencies.

- **Support more research into how these tools impact federally protected groups, especially in terms of the risk modeling/scoring and predictive analytics and also the training of AI systems that are being integrated into workforce management tools.** Previous research on how AI-powered hiring and recruitment products can lead to discrimination against protected classes has been documented. But less focus has been on how these risk modeling tools can also be used to target these workers in a way that can lead to various forms of exploitation and intimidation. This information will be essential in not only increasing regulatory investigations surrounding potential abuses of workers’ biometric data but also help support FTC rulemaking in this area, the increasing number of state-level complaints and class action suits taking place, especially in Illinois where the Biometric Information Privacy Act (BIPA) is the most comprehensive biometric legislation in the country, as well as new regulations and laws emerging in different states.

- **OSTP should encourage the use of algorithmic impact assessments as an industry standard for these products.** The space of algorithmic impact assessments is rapidly expanding and it may provide vendors with practical tools for understanding the impact that their products have on workers. Additional guidance is needed to help employers conduct better due diligence when purchasing and using these products and OSTP can issue guidance to ensure that both vendors and employers are obligated to conduct third party evaluation of their use of these technologies.

Coworker, welcomes OSTP’s leadership in helping to better understand the rapidly evolving field of algorithmic management and surveillance tools.

Thank you for the opportunity to provide these comments.
A contribution for

THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)

Request for Information (RFI):
Automated Worker Surveillance and Management

Inputs for the RFI - EU-based ecosystem of discriminatory employment digital platforms reaching the United States: towards “discrimination by default”?

Overview

Further to the publication of the request for information (RFI) from the Office of Science and Technology about “Automated Worker Surveillance and Management“, the purpose of this contribution is to provide awaited inputs for the RFI and share insights on an emerging ecosystem of EU(France)-based employment-related digital platforms infringing on workers’ rights for a number of years and that has now landed in the jurisdiction of the United States, posing numerous risks to workers’ rights that fit precisely within the scope of this RFI.

After presenting an overview of that ecosystem (Part I°), this contribution will follow OSTP’s Data and research-related questions listed in RFI section 4 (Part II°) to share inputs, either pertaining to that ecosystem or to other automated systems related to worker surveillance.

This contribution will then raise some matters (Part III°) which are, in our opinion, related or could contribute to the subject of this RFI such as: recent NYC bill on automated employment decision tools (AEDT) - employment discrimination against the unemployed & long-term unemployment - bias in employment against financially underserved communities: the example of cyber jobs - US-UK data bridge & potential risk of abusive automated employment blacklisting via the CIFAS EIFD – DoJ recent no-poaching case in Connecticut and the concept of buyers’ cartel in competition law - the recent initiative from US lawmakers against data brokers. This will lead us to address the questions on policies, practices, or standards that could protect workers, as listed in RFI section 5 (Part IV°).

Notice:
As there is a policy to make the content of these contributions public, a certain level of information can not be provided at this stage, such as names of business directly or indirectly involved in the described practices. For the same reason, minimum inputs can be provided at this stage in response to RFI Section 1. about worker’s perspective while answers to this section would bring direct evidence to some of the questions asked in RFI Section 4. Data & research-related questions (and also bring SEC-related topics).
Preliminary considerations - references

This section lists the major regulations, guidelines or other documents considered while preparing this contribution for the OSTP:

1. United Nations - Universal Declaration of Human Rights (with focus, in this contribution, on workers’ rights) 

2. Charter of the Fundamental Rights of the European Union (with focus, in this contribution, on workers’ rights) 


Nb : this recommendation is non biding but as it is used as a reference for data privacy as it inspired, at least in part, national or regional legislation.

4. Blueprint for an AI Bill of Rights

5. EEOC - FTC – CFBB joint statement about AI
EEOC-CRT-FTC-CFPB-AI-Joint-Statement(final).pdf

6. US – EU terminology for AI

7. Digital Employment and Data protection in France : towards “discrimination by default”?  
Provided as attachment to this contribution.

8. TFUE article 101 and 102

9. OECD “Purchasing Power and Buyers’ Cartels – Note by the European Union”, 22 June 2022

10. Definitions of abusive practices according to the Portuguese Competition Authority 

11. Definitions of collusive practices according to the Portuguese Competition Authority 

12. Labour market agreements and competition policy by the Portuguese Competition Authority
Best Practices In preventing Anti-competitive Agreements in Labor Markets 

13. Proceedings from the European Commission against Amazon's marketplace (France, Germany, Spain)

14. NYC bill on AEDT

15. Decision in no-poaching case from the DoJ brought to the District Court in Connecticut
I°) Overview of the ecosystem of discriminatory employment platforms

A°) Introducing the ecosystem

[1]. The ecosystem relies on a number of “dual mode” websites - on one side, a candidate/worker platform and on the other side, a business-to-business (B2B) platform - where features or use cases have been recorded to infringe on workers’ rights by unfair or misleading data collection or sharing practices - not known to workers - up to the point of features causing them a high risk of discrimination, if not directly denying their “Right to work”, as defined in article 23 of the Universal Declaration of Human Rights [Ref. 1], or the professional freedom & right to work, as defined in the EU Charter of Fundamental Rights [Ref. 2]. These processing activities of personal data also appear to breach key privacy & data protection principles, such as those defined in the OECD since 1980 [Ref. 3] or other regulations.

[2]. Furthermore, at least some of these platforms provide features that may infringe on antitrust / competition law, for instance, by enabling horizontal collaboration among hundreds of IT service companies that are otherwise supposed to be competitors. Practices in that ecosystem may also be considered collusive or breaching other provisions of applicable competition law.

[3]. That ecosystem, nested in the 150+ billion euros French digital industry, has been impacting workers rights and creating barriers to entry to the IT service market in France for many years – for instance one of these platforms appears to have been set up back in 2013. However, since 2020, a growth acceleration has been recorded in their activity and at least two of the identified platforms are now based in or claim to be operating on the American market.

[4]. The practices enabled in that ecosystem pose serious risks to workers, including to their health and safety, equal employment opportunities, privacy, ability to meet critical needs and exercise of workplace rights; these practices also appear to breach multiple laws at state level prohibiting employment blacklisting practices. As such, we also believe that these practices go also against the Administration’s commitment to ensuring that all workers have access to high-quality, well-paying jobs, including jobs with opportunities to organize and bargain collectively with their employers through labor unions, as articulated in the Executive Order 14025 (Worker Organizing and Empowerment) 6 and through a competitive market for their labor, as articulated in Executive Order 14036 (Promoting Competition in the American Economy).

B°) Facts and findings

[5]. The following paragraphs are based on the preliminary report titled “Digital employment in France and protection of personal data: towards “discrimination by default”?, published in French on 13 July 2021, and translated in English on 4 August 2021 [Reference 7].
To start with a general and quick typology of sites related to digital employment / recruitment, dealing with publication of job adverts to collect applications from candidates, we can say that this type of websites and platforms fall into five main categories (not exhaustive):

(i) Career pages of employers / contract jobs providers websites (large groups, IT Services, SMBs, startups, public employers, etc.);

(ii) Recruitment companies websites, serving employers from the above category (i);

(iii) Resume libraries (or cv libraries), which are sites where candidates can apply to job postings published by employers (i) or recruiters (ii);

(iv) Job/assignment aggregators, which gather published offers that may come from websites in categories (i) to (iii), and even sometimes (iv);

(v) “Marketplace” platforms, which have various features and can interact, in different ways, with sites belonging to the four previous categories as well as to the category (v) itself.

This first typology is not exhaustive, does not intend to include all types of sites or platforms in SaaS mode related to employment (eg. Application Tracking Systems, “ATS”, or s tools with a single specific purpose), but aims at removing a first level of opacity since it is easy to confuse these marketplaces with the four previous categories of websites whereas their features and objectives are radically different.

Once such a typology has been established, the main distinction to be made in order to measure the actual scope of the types of personal data processing carried out by the "marketplaces" as well as their effects, consists in distinguishing them from classic cv libraries.

In summary:

- In a cv library or similar websites, candidates put their resumes online to share them with employers or to apply for job offers. Employers and recruiters only have access to the information input by the candidates and shared by the latter with the recruiters at the time of an application. CV can be found by employers or recruiters when candidates agreed to find them with a search. As far as job applications data is concerned, this is therefore a one-to-one relationship between the candidate and the employer/recruiter;

- In the "marketplaces", employers and recruiters have access to various functionalities that allow them to collaborate with each other, rate candidates or make comments on their resumes or profiles, etc. This totally distorts the relationship between candidates and employers or recruiters, since employers and recruiters now act as a "block" and share data with each other without the knowledge of the people these data pertain to.
Most problematic use cases identified within this ecosystem of marketplaces

The following problematic use cases have been identified in that ecosystem for now:

• Candidate profiles can be created without the consent or even the knowledge of the interested persons – they can be abstracted and managed as mere products;

• Evaluations / "vetting" of candidates not known to them but visible to all employers / recruiters accessing the platform;

• Comments by employers / recruiters on candidates' cv's without their knowledge;

• A non-public market of resources (consultants), involving hundreds of IT Services companies supposed to be competitors sharing commercial information such as price and appearing to act as one undertaking – nb: one platform doing such business in the most obvious way appears to have recently refocused on the French market only.

• Obstructing access to employment by providing inaccurate or false, (quasi) eliminatory or discriminatory information;

• Explicit function of "disqualification" (aka « blacklisting ») of candidates not known to them but visible to employers / recruiters accessing the platform.

Breach of the principle of Openness (OECD) or Transparency (GDPR)

The openness principle from the OECD framework is defined as follows:

“There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.”

The above listed use cases recorded on these marketplaces breach this principle, as a significant if not the main purpose of their usage is not made explicit to the workers or candidates.

Breach of the principle of Collection Limitation Principle (OECD)

The Collection Limitation principle from the OECD framework is defined as follows:

“There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.”

When such a platform creates profiles about data subjects without their knowledge or consent, that platform appears to be also breaching the principle of Collection Limitation principle.

The *Purpose Specification* principle from the OECD framework is defined as follows:

“The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”

This principle is for instance breached in this ecosystem when personal data from natural persons that are collected at the time of an application appear to be made available or at least known to third parties other than the company or recruiter these natural persons applied with.

[12]. Breach of the principle of *Necessity* (GDPR)

The uses cases listed in section [8] also breach the principle of necessity, as it can’t seriously argued that all the employers or recruiters dwelling on one of these platforms need or even would have a legitimate interest to know about such a broad set of data about an applicant.

[13]. Breach of the principle of *Proportionality* (GDPR)

The uses cases listed in section [8] also breach the principle of Proportionality, as for instance, allowing that comments made on a candidate’s profile or resume, linked to one specific application or job experience, be broadcast to hundreds or thousands of business client of such platform has disproportional consequences on the employments rights of these natural persons.

[14]. Use of automated systems to produce rankings of “best candidates” at marketplace level

These platforms also claim to provide to their clients – employers or recruiters – the “best candidates”, the “best talents”, etc. This means that these platforms are profiling candidates and/or producing an assessment. While such mechanisms existed for individual applications – and can result in discrimination -, what raises even bigger serious concerns is that such rankings appear to be produced at the marketplace level, which means that this ranking will impact candidates not for one specific position or application, but at the scale of that part of the employment market.

Moreover, in light of the serious risks of breaches of fundamental privacy / data protection principles already presented in sections [9] to [13], the fact that this ranking is produced without any transparency or even information as to how such ranking or selection is produced.

If questioned, a typical answer these platforms may put forward is that they “didn’t disadvantage anyone” but this doesn’t suffice : if they promote always the same profiles to be on the “top of the pile”, this type of processing is known, on other types of marketplace, to strongly influence the decision-making process, and result in a recurrent disadvantage to the candidates who, for whatever reason, wouldn’t be put on top of the list but at the back of it.
A further examination of these use cases and the associated risks of breaches or breaches already presented would be also very likely to show:

- a lack of assurance as to the principle of Data Quality (OECD) or Accuracy (GDPR);

- an extended risk of bias, “by default”, as broadcasting that nature of data about workers or candidates represents another significant factor of influence through the concept of bias, such as confirmation bias or anchoring bias among employers and recruiters on these marketplaces;

- increased risks for vulnerable candidates, such as those or coming from underserved communities who are less likely to get access to employment by knowing employers directly and therefore would have to submit their resumes and application via that kind of websites instead, with all that it involves in terms of additional risks of discrimination;

- a context reducing if not nullifying workers’ actual bargaining power while implementing, at the same time, a ground that favors employers’ and recruiters collusive practices in hiring, wages setting or other aspects;

- an opaque online space suitable for covert harassment of targets, such as former employees who resisted various types of abuse in the workplace or whistle blowers for the public interest, who could be retaliated against while the lack of transparency makes that targets can’t even suspect that such practices occur on websites deemed to be supposed to provide employment.

Blacklisting / automated elimination of blacklisted applicants

These platforms appear also to be enabling, directly or indirectly, features that result in to “blacklisting” of consultants, workers or candidates.

*Nb : as a side note, we know that, for instance in technology, companies in the United States such as Red Hat are taking care to use inclusive terms and replace words such as “whitelisting” or “blacklisting” in the context of networking security by equivalent expressions such as “allow list” or “block list”. In the specific context of employment discrimination, this word is still kept as it is frequently the one used in US state laws to prohibit such practices.*

In the two platforms referred to earlier in this contribution, we have recorded that:

- in the first platform, a feature is providing a check box “freelance disqualified” (in French);

- the question of blacklisting was also asked to the second company, which declined to answer.

Across the United States, numerous local laws prohibit employment blacklisting in various ways and terms.

The legal information website nolo.com has been publishing, for more than five years, a list of laws prohibiting blacklisting in about thirty states.
This list of US laws applicable across the country can be found at the following URL:

Based on this list of laws and the summary of their content, we have made a high-level review comparing these laws with the practices recorded in the platforms of that ecosystem that are now based in the United States or claim to be operating there.

The outcome of this review is attached as an annex to this contribution (4 pages) and tends to show that more than twenty states in the US may already have laws in place that could tackle such blacklisting practices, including states with major economic activity such as:

- California;
- Florida;
- New-York;
- Texas.

[18]. As a side note, there is also a law prohibiting blacklisting in Connecticut, where a very recent case brought to court by the Department of Justice (DoJ) has been judged in matters related to no-poach agreements. This will be further discussed in part III°) of this contribution.

[19]. In conclusion to this section, the research undertaken on this ecosystem that has been operating in France and in the EU for years, and that has landed recently in the United States:

- violate candidates’ rights to privacy and data protection, both in the EU and in the United States;

- impact workers’ rights to be fairly considered for work, enabling marketplace-wide bias or discrimination and even engaging in illegal blacklisting practices;

- provides a setting compatible if not required to engage in labor fixing, wages reduction to the prejudice of all citizens impacted by the outreach of these platforms, in the EU and in the US alike;

- creates opaque conditions not required for fair access to work, increasing risks for the more vulnerable candidates, including from underserved communities, and may even serve as a place for covert harassment or retaliation against former employees or candidates, including against whistle-blowers.

[20]. As those two platforms are positioned at different levels, addressing different markets although with an overlap (the first one focuses more on large corporate end-clients, such as financial services or banks; the second one addresses various industries, but seems to be more focused on start-ups), further research could be useful to further detail the extent of their anti-competitive practices that are providing an unfair advantage to their cartel(like) members against new entrants, businesses respecting fair competition but, before all, on the labor market.
II°) Data and research-related questions asked by the OSTP

a. What data and evidence exist on the prevalence of automated worker surveillance and management systems across different industries, occupations, and regions, including changes over time?

Firstly, we would like to detail or restate – just in case – why we consider that the discriminatory employment platforms are one kind of automated worker surveillance and management systems, and most probably a significant one.

This is because these systems, embedding various kinds of automated processing of personal data, are:

a°) the places where workers and candidates will more and more have to go to find and apply for work: their growth is accelerating, and what could be a niche a few years ago becomes an industry on its own;

b°) websites that are, in general, consumers of multiple online services – often vaguely referred to in privacy notices - that are themselves often based on automated systems. These online services would typically include resume/cv or degree online verification, credit check, or other forms of evaluations, more or less valid or automated, but still that can be shared online or used as inputs to produce for instance the marketplace rankings of candidates, as presented in the section [14] here above.

As such, this type of platforms acts both as the gate keepers of access to work, and as a place of choice to act as an aggregator of outputs produced by other automated worker surveillance and management systems. This feeds into question “i” herefater.

Then, as far as the ecosystem described in I°) is concerned, these platforms have a focus on digital employment but that kind of practices has spread to websites advertising jobs for any type of occupation, industry or region.

These websites share publicly the names of some of their largest clients, and these companies operate in the following industries (as listed in the attached report on discrimination by default):

- Telecoms
- E-commerce
- Retail
- Consumer goods
- Start-ups
- Services
- Industry
- Transportation

The above facts are documented and further evidence can be shared upon request.

Please note that, while evidence can’t be provided for the industry of temporary work, similar practices would take place there as well.

While raising awareness on these platforms with a workers’ union representative back in June 2020, this person told me that he heard similar practices would exist in the temporary work
industry, but he added he never managed to get evidence of it, as these practices are covered by a climate of secrecy among managers and hiring staff. But the effects on workers’ rights that I have been told about were similar to the ones resulting from the practices are now documented.

Back to the two platforms present or claiming to operate on the US market, these are focused on so-called “freelance” workforce, which may, depending on the type of assignment, its relation to hierarchy in the commissioning organization or local regulations correspond to genuine provision of services or mere substitution of salaried workforce.

**b. What data and evidence exist on the impact of automated worker surveillance and management systems on workers, including workers’ pay, benefits, and employment, physical and mental health, and ability to exercise workplace rights?**

The practices identified and described in part I°) strongly suggest:

- that such automated workers surveillance and management systems introduce “discrimination by default”. As a consequence, they impact workers’ rights in many ways, starting with chances to get employed but also get a fair wage [see section 15.];

- that on one hand, candidates who get on “the top of the pile” [see section 14.] will get jobs, while those discriminated will incur incremental, self-repeating degradation of their professional prospects, directly impact their incomes, pay, benefits and health.

This impact on workers’ rights will be all the more severe that most workers are not informed of - or even don’t believe in – practices that go as far as blacklisting, many targeted workers or candidates who be likely, in turn, to feel personally affected by these repeated rejections without understanding them. Needless to say that the less favored communities are, here again, likely to be the most impacted with regards to unequal access to other ways to get work or relief.

Research data to get an objective and factual understanding of these impacts might be gathered with the help of various federal administrations such as the tax administration – as far as personal data may be used in the United States, once anonymized, for a research of public interest. Such data could be then used to define groups (clusters) of businesses, platforms or recruitment companies with different level of adoption of automated surveillance technologies and then, observe incomes, career evolution etc. of their employees, considering various factors (see question “d”). This could be joint initiative between OSTP and EEOC, FTC and/or CFPB.

**c. What data and evidence exist on the impact of automated worker surveillance and management systems on labor rights, including workers’ abilities to form and join unions and bargain collectively with their employers?**

In our understanding, these platforms are the exact opposite of workers’ rights, as they represent a space that strongly favors employers’ if not organizes buyers’ cartels or even a monopsony.
Centralized databases enabling, directly or indirectly, employers or entities representing businesses’ interests to discriminate against or even to blacklist have been used to target members of workers’ unions or any worker raising concerns about health & safety, or any other valid concern. This was the case in the construction blacklist identified in the UK in 2009, which mingled such illicit blacklisting records with rather rare cases which should be dealt with by law enforcement, and not by a private database.

This construction blacklist destroyed thousands of lives over periods of time going from eight to twenty years, destroying families, communities and causing even deaths. This scandal is described in the report on discrimination by default [Ref 7, page 4 & 5]. Although these facts go back to 2009, further alerts from workers’ groups or union in 2014 or later spoke of new occurrences of similar blacklisting practices. As part of this contribution, we will also mention the case of the CIFAS EIFD, a UK-based database allegedly designed against organized, internal fraud in companies but which seems to whitewash blacklisting practices. In light of the new US-UK data bridge that has been agreed, this kind of automated system may get soon a footprint in automated workers’ surveillance and management in the United States [see III°].

Another sign that documents that these discriminatory employment platforms undermine workers’ right and are contrary to the rights of workers to organize is what happened when we brought these practices to the knowledge of the French Data protection authority, in 2019 then in 2020, to several decision-makers in that authority. No action was taken to investigate these practices, or even to properly acknowledge the whistle blowing done about this matter of public interest. However, after we contacted some workers’ unions in France in September 2020, one of them responded by offering their support on this matter but soon after, communications were cut. We realized one month later that the French DPA didn’t investigate the discriminatory platforms but chose to control workers’ unions instead.

https://www.cnil.fr/fr/fichiers-dadherents-un-syndicat-quelles-sont-les-bonnes-pratiques

This type of targeted control compared with deliberate *laisser-faire* in favor of automated surveillance & management systems appears as a clear hindrance of labor rights, and also echoes the hostile climate towards social, racial and workers’ rights in the country, as recently raised by the United States and some other European countries before the United Nations.


d. What data and evidence exist on how the impact of automated worker surveillance and management systems differs across groups of workers, including based on characteristics such as race, national origin, sex, age, disability, religion, or health status?

We believe this question could be addressed in the same way and as part of the research approach identified in question “b” here above. The factors mentioned to in “b” implicitly referred to characteristics such as race, national origin, sex, age or home addresses / areas, which may indicate or be linked with social or economic uniformity. For characteristics such as disability, religion, or health status, we are unsure how it is possible to access anonymized, aggregated data but the principal to produce evidence would be similar as for question “b”.

11/23
e. **What data or evidence exists on whether automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination?**

We believe that our research about this ecosystem of employment platforms shows that these instances of automated worker surveillance and management systems are being used for discriminatory purposes or resulting in discrimination.

This can be further researched, in this ecosystem and in other types of automated worker surveillance and management systems.

To take one example, it should be feasible to check if Application Tracking Systems (ATS) or some of them, produce outputs that show discrimination.

Considering one protected characteristic - for instance, race or national origin – it could be possibly easy enough to identify relative differences between ATS as to the number of applicants with these characteristics and the number of selected candidates for interviews, and those actually landing jobs.

As data needed to find out about these results could be anonymized and aggregated, it might be possible to access such data for a research in the general interest.

f. **What data and evidence exist on whether automated workers surveillance and management systems impact employers’ ability to recruit and retain workers?**

That’s a very interesting question, and while this contribution is focused on workers’ rights, we also believe that many employers may not be aware or realize what results get actually produced by automated systems, which are often working in a fairly autonomous manner.

Promises made by vendors of automated workers surveillance and management systems may not live up to the results of real tests, when such tests are carried out in an inquisitive way, such as the ones the MIT did for some AI interview tools. [https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/](https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/)

Employers may be misled by automated tools, especially when results of such tools are presented by vendors as scientific while they may actually be the output of simple, if not simplistic computations based on a few or even one Python function, for instance to compute the distance between two vectors made of word to declare a “match”. Such computation, as many others, may produce both false positives and false negatives.

As a result of the above, we believe that focused scrutiny of Federal agencies on at least some high risk or dubious types of automated workers surveillance and management systems could give incentive to vendors to deliver systems that bring genuine value to employers, while respecting workers’ right and minimizing risks of discrimination.
g. **What data or evidence exists on how the provision of reasonable accommodations is accounted for in the design and operation of automated worker surveillance and management systems?**

We don’t know that matter enough to provide specific inputs, but we believe that an approach combining elements outlined in questions “b”, “e” and “f” could be applicable.

h. **What data and evidence exist on why employers decide to adopt automated worker surveillance and management systems?**

We are unaware of such data today, but from various articles of press, employers decisions to adopt such systems may stem from:

- willingness for better efficacy or efficiency;
- concern to lag behind competition if not using the same tools;
- concerns about unethical or illegitimate actions from employees;
- efforts to reach more objective decisions, or to reduce bias by using more scientific approaches.

Such drivers could be further investigated by a direct survey with employers, or research on vendors website. Analyst firm, such a Gartner or Forrester could also provide valuable inputs.

i. **Are there any existing or new systems that aggregate worker surveillance data across multiple employers?**

The aggregation of those data is especially concerning, and this is precisely one of the concerns that we have because of the ecosystem of discriminatory platforms presented in part I°) of this contribution.

We are afraid though that this practice – to share applicants’ and application data even with companies or recruiters who were not the intended recipients of those applications – is not an isolated fact, as one ATS based in the United States brings forward the fact that they don’t engage in such practice as a proof of an ethical way to manage applicants’ data.

j. **What are new or emergent automated worker surveillance and management systems—or new and emergent uses of existing technologies—that Federal agencies should be tracking?**

In our opinion, Federal agencies could be tracking automated systems in a number of use case, or markets or circumstances. These could be defined upon strategic considerations and priorities adopted by each of these agencies or in joint initiatives – such as the joint initiative from the EEOC, FTC and CFWB on AI.
Just to name of few of those use cases, this tracking could deal with systems claiming to do:
- cv/resume or qualification verification and the sharing thereof;
- checks and / or management of so-called anti-fraud or internal fraud databases, other that official sources and including databases located abroad;
- assess undefined traits, such as “cultural fit” of candidates or workers, which may typically increase risks of discrimination or bias;
- any of the kind of AI processing activities confirmed as “high-risk” in the AI Act text that was just presented in the EU parliament.

An input that would be very useful for this question would be to start from an inventory of the main categories of automated worker surveillance and management systems – please see next question “k”.

k. Where might further research, including by the Federal government, be helpful in understanding the prevalence and impact of automated worker surveillance and management systems?

Further research might be helpful in understanding the prevalence and impact of automated worker surveillance and management systems such as:
- getting an overall picture or an inventory of the main categories of automated worker surveillance and management systems;
- split each category into classes to get a finer understanding of prevalence and/or impact;
- identify the drivers – see question “h”;
- further analysis to get objective data on actual levels of systems maturity or efficacy;
- observe changes and evolution over time.

This might be seen as high-level road map, that can be of course further detailed.
III°) Matters related or that could contribute to the subject of this RFI

A°) NYC bill on Automated employment decision tools (AEDT)

A new bill issued by the NYC Department of Consumer and Worker Protection (DCWP) regarding Automated employment decision tools is effective since January 1, 2023.

On DCWP official website, this bill is summarized as follows:

This bill would require that a bias audit be conducted on an automated employment decision tool prior to the use of said tool. The bill would also require that candidates or employees that reside in the city be notified about the use of such tools in the assessment or evaluation for hire or promotion, as well as, be notified about the job qualifications and characteristics that will be used by the automated employment decision tool. Violations of the provisions of the bill would be subject to a civil penalty. Read Local Law 144 of 2021.

Note: DCWP will begin enforcement of this law and rule on July 5, 2023.

We welcome the bill and consider it sends a signal to support responsible use of automated systems in the field of employment. This is of course with the understanding that this bill regards automated systems, which by default suggests a high risk.

Our understanding is that, following request for comments from the public, which included employers, a change has been introduced in the bill so that the auditor leading the bias audit of the system may exclude from this audit “a category that represents less than 2% of the data being used for the bias audit from the required calculations for impact ratio”.

We believe that this changed provision may open the door to significant risks of discrimination, and the fact that such exclusion would have to be justified by the auditor does not, in our opinion, bring sufficient safeguards.

Excluding a category representing 2% of data can:

- hide or hinder proper understanding of a bias that regards a minority group corresponding to a characteristic such as race, national origin, religion, etc.
- hide or hinder proper understanding of a bias that regards a group not frequently seen or considered in applications, eg. unemployed, long term unemployed or whistleblowers, who might be screened out from the earliest stages of the automated decision-making and not easily noticeable as not tracked in the same way as protected characteristics;
- a 2% bias affecting a category could also reveal in fact the “tip of the iceberg” of a product flaw generating in fact a broader bias or risk of discrimination
- it gives also a non negligible discretionary power to system auditors who may be exposed to various level of pressure.

These remarks lead us directly to the known bias or discrimination against the unemployed.
Known bias or discrimination against the unemployed, including long-term

The bias from recruiter and employers against the unemployed is not new and a known factor in the hardship experienced by numerous job seekers even when jobs suitable for their profiles are available.

Such bias or discrimination is harming communities, even more those who are the most exposed to economic hardship or unemployed, and initiates a vicious circle which, if not quickly interrupted, leads people to become long-term unemployed which is often presented as an “objective” reason to reject an application.

Back in 2011, during the tenure of the Obama – Biden Administration, attempts were made to protect the unemployed by law, in order to make unemployment an additional protected characteristic.
https://www.huffpost.com/entry/obama-jobs-plan-bridge-to-work-program-long-term-unemployed_n_953838

This effort was strongly opposed by some business groups, and a new initiative to support the long-term unemployed was put forward by the Obama – Biden Administration in 2014, which succeeded to put in place a voluntary pledge from many companies to support the initiative.

The main points here are:
- there is a persistent bias and discrimination against the unemployed when they apply;
- this bias, if not quickly interrupted, automatically leads to long-term unemployment and hardship of those deprived of work;
- this kind of discrimination or bias is very easily set in automated employment decision tools: eg. resumes / cv’s showing a gap after the last identified work position can be screened out after “x” weeks or months, or even immediately.

This bias can be openly noticed in recruitment forms asking for availability for candidates, that don’t include an option such as “immediately available” or “available now”.

We believe that this criteria should be scrutinized in AEDT, as this bias harms the rights of workers, increases the costs of unemployment for the community while not bringing evidence that unemployed candidates would be less productive or efficient that those in jobs.

27 weeks is a short time span in the life of a business, even if that business is an AI vendor. 27 weeks is also the duration after which an unemployed person is considered as a long-term unemployed. Especially in the current economic context, we believe that there is an urgency to ensure that AEDT and other automated workers surveillance and monitoring systems don’t discriminate against the unemployed people, as more and more people are just a few paychecks away from financial hardship, which can be another obstacle to get in employment.
Known bias or discrimination against financially underserved communities – example to access cyber jobs in ISO 27002

Performing a credit check can be part of many employment decision-making processes and this can be understandable in a number of situations. However, as many “screening” steps get automated and often without the required transparency and openness towards applicants, it can nullify in practice the recommendations or rights to know any adverse or negative information. [https://consumer.ftc.gov/articles/employer-background-checks-your-rights](https://consumer.ftc.gov/articles/employer-background-checks-your-rights) [https://www.ftc.gov/business-guidance/resources/background-checks-what-employers-need-know](https://www.ftc.gov/business-guidance/resources/background-checks-what-employers-need-know)

To take an example, performing a credit check is explicitly mentioned in the standard ISO 27002 in the HR section pertaining to the hiring of cybersecurity professionals. The reasoning behind the requirement seems to be that adverse information in a credit report would either reveal lack of professional skills or present a risk for corruption or for bribery. While this assumption may not be always wrong, we believe it is strongly bias against underserved communities as it suggests a strong link between financial prosperity of an individual and his or her integrity. Cases when massive fraud, bribery or corruption was committed by wealthy individuals are not exceptions.

And just as for unemployed people, this process creates a vicious circle where people in financial hardship get refused access to employment, while getting employment would in fact resolve their hardship and put them on the way to prosperity.

As with the bias or discrimination against the unemployed, we believe automated credit check or similar automated steps – which may in reality be mere outdated information made available through data brokers but that is still regarded as current or genuine – create high risk for discrimination, go against policies such as the one to support Americans to get access to “high-quality, well-paying jobs, including jobs with opportunities to organize and bargain collectively with their employers through labor unions, as articulated in the Executive Order 14025 (Worker Organizing and Empowerment) 6 and through a competitive market for their labor, as articulated in Executive Order 14036 (Promoting Competition in the American Economy)”.

We believe that addressing this bias or discrimination based on financial situation in automated systems would be in the public interest, to support the above policies and it seems especially relevant in professions such as in cybersecurity where there is a strategic and urgent need to recruit. [https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html](https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html)

US-UK Data bridge & potential risk of automated blacklisting via the CIFAS EIFD

The very recent announcement of the US – UK Data Bridge opens new opportunities for business between the two countries bound by the special relationship. The data transfer are
essential to many industries and we would like to raise here awareness about a specific risk that fits within the scope of this RFI.

Without making a call on respective qualities of data protection and privacy regulation in different countries and on other legislation applicable in the context of international data transfer – which is very broad and complex, it is reasonable to state that there may be a tendency among businesses to outsource remotely the provision of services they may know as questionable or even illegal, as an implicit obstacle to the exercise of worker’s rights.

As such, “screening” services mentioned in privacy policies are not only defined vaguely in terms of scope, but also in terms of location. For workers with limited financial resources and network, accessing legal advice overseas is indeed an obstacle.

Having taken the above under consideration, we believe that an increased flow of personal data can enable more remote “screening” services, including automated ones, and in this context, there is a significant risk if US based recruiters or employers access the CIFAS EIFD.

The EIFD is a specific database hosted by the CIFAS, which had previously a mission against fraud in financial services (National Fraud Database) or other databases that we do not address here. The Enhanced Internal Fraud Database is supposed to fight organized fraud, while according to CIFAS own staff, 80% of records are not related to that kind of fraud. This database has been extended to include now “employment application fraud”, and an inaccurate resume / cv is enough to get a record as a “fraudster”. Markers are kept for six years and having a record means that applications get rejected, without any hearing or cross examination.

As additional information, we are providing the following URLs:

- the CIFAS EIFD presented itself as a “benefit” to its members
  https://www.cifas.org.uk/fraud-prevention-community/member-benefits/data/ifd
- the list of CIFAS EIFD members
  https://www.cifas.org.uk/services/internal-fraud-database/internal-fraud-database-members
- an article published by a legal UK firm mentioning the misuse of CIFAS by employers
  https://www.msbsolicitors.co.uk/our-expertise/commercial/cifas-marker-removal/
- as a matter of comparison, we add the link to the “Violation tracker”, a research project based in the United States and tracking violations committed by corporations and their leadership – although those serious violations seem not being tracked in automated verification systems described above in C°) and in this section D°).
  https://violationtracker.goodjobsfirst.org/

We believe that the use of such so-called “internal fraud” service by automated worker surveillance and management systems would cause a high risk to workers’ rights, via a blacklisting system not providing genuine safeguards such as a right to be heard or even informed in the 80% of case that are not linked to the organized fraud it is supposed to tackle.
E) DoJ recent no-poach case in Connecticut and the concept of buyers’ cartel in competition law

This subject is a very complex topic, and the court decision recently taken shows the enormous work done by the Department of Justice.

While we do not claim knowledge in the field of US competition law, we would like to share the following with regards to the decision taken on 28 April by the District court of Connecticut, under No. 3:21-cr-220 (VAB), as it may be related to organized labor discrimination outlined in part 1) of the present contribution and also in other settings.

The decision taken in this case has been summarized in a media as:

a) The DoJ argued that the rule of reason didn't apply in this case because the no-poach agreement constituted a horizontal market allocation, where competitors at the same market level structure a labor market in order to minimize competition. However, the corporate executives said it wasn't a horizontal market allocation because it involved a vertical commercial relationship between the manufacturer and its outsourced providers.

b) The court concluded the no-poach agreement was not illegal because the hiring restrictions frequently changed and allowed for exceptions, which suggests that often hiring was permitted, sometimes on a broad scale. “No reasonable juror could conclude that there was a cessation of meaningful competition,” the court stated.

From a high-level reading of the decision, we understand the case as presented by the DoJ, and notice where the defendants appear to be circumventing the real issue which actually seems to be a horizontal cartel, as named by the DoJ, which acts as a kind of buyers’ cartel, which is characterized in an OECD report titled “Purchasing Power and Buyers’ Cartels – Note by the European Union”, 22 June 2022 [Ref 9].

Page 8:
“According to the report, in the case of a buyer cartel, undertakings agree with one another on how they will individually interact with suppliers, or they exchange commercially sensitive information with one another about how they will individually deal with suppliers, thus removing competitive uncertainty that would otherwise have existed between them.”

Page 10:
“The distinguishing factor between a genuine purchasing agreement and a buyer cartel is whether the buyers, be it together or through a type of intermediary, collectively negotiate and conclude an agreement with a supplier. Conversely, if each buyer interacts individually with a supplier while coordinating its behaviour with other buyers, for example on their price negotiation strategy or through exchanges on the status of their individual negotiations, this amounts to a buyer cartel. In other words, the distinguishing factor is whether buyers present themselves jointly to a supplier in their negotiations or purchases or whether they seemingly act individually but nevertheless coordinate their behaviour with other buyers.”
If the same competition practices may be applicable to a buyers’ cartel interacting with suppliers as well as to an employers’ cartel interacting with employees, could we imply that:

- a vertical relation doesn’t exclude the existence of a horizontal cartel in its frame;
- the decision shows that the competitive uncertainty between employers has been removed;
- the employers interact individually with the employees while coordinating with other employers.

This kind of process is, we believe, precisely what is impacting workers’ rights as shown in 1°).

**F°) US law makers raising questions to data broker**

In this section, we are sharing the information read in the press about an initiative taken by US law makers to bring more transparency about what happens in the data broker industry.

Data shared, sold or provided to third parties by any other mean could also be used as inputs, or receive inputs, aggregated or not, from automated worker surveillance or monitoring systems.

The following URLs provide a press article and the full letter sent to one of these data brokers.


https://d1dth6e84htgma.cloudfront.net/05_10_2023_Acxiom_Data_Brokers_Letter_1cbb81da32.pdf?updated_at=2023-05-10T16:19:56.031Z

We believe that the fifteen first questions could be also helpful to address the matters related to automated worker surveillance and monitoring systems, and we look forward, hopefully, to reading in the media the answers sent by these data brokers in response to the concerns raised by the US law makers on data protection & privacy of citizens.
IV°) Policies, practices, or standards that could protect workers (RFI section 4)

A°) Foreword: the five principles of the blueprint for an AI Bill of Rights

The AI Bill of Rights introduces five principles:

1. Safe and effective systems
2. Algorithmic discrimination protections
3. Data privacy
4. Notice and explanation
5. Human alternatives, consideration, and fallback

We believe that these principles provide a powerful yet accessible framework to scope and address major areas pertaining to AI and, whenever possible, we will use these principles as goals of the suggested policies, practices or standards that could protect workers.

B°) Thoughts about policies, practices or standards that could protect workers

a. What guidelines, standards, or best practices might inform the design of automated worker surveillance and management systems to protect workers’ rights?

- As far as violations of labor market are concerned, in terms of competition, we believe the following resources about labor market agreements and competition policy by the Portuguese Competition Authority might be useful when considering practices “imported” to the United States from the EU and that can harm worker rights here too.

  Best Practices In preventing Anti-competitive Agreements in Labor Markets

- Items listed in below question “c” – a) regulation: may also be translated into standards or guidelines to assist vendors, employers or recruiters to comply with the proposed regulation.

b. Are there policy approaches to regulating automated worker surveillance and management systems from State, Tribal, territorial, or local governments or other countries that Federal agencies could learn from?

- we believe that the right of workers, as defined in the Universal Declaration of Human Rights, provide an overarching reference that may be easy to use and powerful at the same time to regulating what these automated systems may or may not do:

- there is a Fundamental Rights Impact Assessment developed in the Netherlands which provides a very detailed and practical framework to ensure responsible AI, which could also be
c. What policies or actions should Federal agencies consider to protect workers’ rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?

a) regulations

These suggestions may address some of the risks or breaches presented in I°), II°) and III°)

- As discussed in III°) A°), we believe that fixed thresholds accepting a given level of bias, as the 2% bias tolerated in the NYC AEDT bill, may cause significant risks to minorities, protected categories or categories at risk of discrimination but not protected (unemployed, long-term unemployed, whistle blowers) of being discriminated, with automated, repeated and incremental harm that could quickly lead impacted people into dire hardship;

- As discussed in III°) B°), we believe that automated system, especially those taking decisions about access to employment (“screening”, “vetting”, ATS review, cv “verification”) should be scrutinized to ensure they don’t act as “firewalls” blocking access to work against categories such as the unemployed;

- As shown in III°) C°), ISO standards such as ISO 27002 in cybersecurity may be broadcasting the idea of credit checks as a panacea for recruitment, we believe such standards could be reviewed on that matter, to a°) remove this recommendation when it is not absolutely required and/or b°) remind or specify what credit check results actually means and remind the right to a hearing, as outlined by the FTC since 2014.

- In Privacy notices, all these automated systems should be explicitly named and their work presented in terms that are fully understandable to the intended audience;

- We think that consent should not be admissible as a legal basis to collect or process PII in the context of work application, including when workers apply for new positions with their current employers

- forbid data sharing of applications made by a natural person with other recipients than the recruiter or the employer recruiting for that specific employment opportunity;

- forbid “digital pillorys” where employers or recruiters may comment cvs or profiles of candidate in front of other recruiters or employers, but without knowledge of the workers;

- demand that any cv, diploma or other verification automated systems be brought to the attention of candidates so that they may have a chance to be heard about any potential discrepancy (FTC’s “right of hearing”)

– right to access & rectify inaccurate employment related personal data / PII, within time lines that are shorter than the time when a person becomes long-term unemployed which is used as a
b) enforcement

- create a system or process of enforcement, with a speed and level of fines that provides
dissuasion to dishonest employers, which would also bring an incentive for honest or compliant
ones;

- [unsure if this item should be in the “enforcement” or “regulation” as it could match either
or both categories] The United States took a number of initiatives to reinforce cybersecurity
and resilience, such as the initiative to improve the software supply chain:

  Link to the Executive Order: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

  Link to online form from CISA: https://www.cisa.gov/secure-software-attestation-form

We believe that this kind of approach applied to the ecosystem of automated worker
surveillance & management systems would help to support Executive Order 14025 (Worker
Organizing and Empowerment) and through a competitive market for their labor, as
articulated in Executive Order 14036 (Promoting Competition in the American Economy)” in
order to realize the awaited benefits for the public good.

Getting interfaces with vendors, employers or recruiters might also be facilitated by introducing
a solution similar to the security file:

  security.txt: Proposed standard for defining security policies (securitytxt.org)

For instance, the above steps would help prevent threat and risks to the plan issued by the FTC
to address abusive use of non-compete agreements and the 300 billions USD lost for the US
economy and prosperity

1

c) grantmaking

- we believe that grantmaking could support independent research projects, which would be
helpful to accelerate the discovery of the ecosystem and practices in terms of data sharing and
automated systems. Since March 2021, we have made an initial proposal for a research project
proposed in Europe titled “Employment Data and Challenges to Individuals’ Privacy
Rights”, which could assist in addressing the sources and scale of risks to workers rights, as
well as identify potential solutions.

Overall, one of the priority would be to establish an inventory or observatory to stay on top of
emergence of solutions, and ensure or anticipate needed rules, regulation or guidelines be ready.

Further information can be shared upon request.

1https://www.promarket.org The Ties that Bind Workers to Firms: No-Poach Agreements, Noncompetes, and Other Ways Firms Create and Exercise Labor Market Power, by Evan STARR, January 3, 2022
2023 Survey
Employee Productivity Surveillance Technology
Executive Summary

Key Findings

The prevalence of EPST

Honor code: IT staff are uncomfortable deploying surveillance tech

Transparency essential, but lacking

Taking a stand

What’s at stake: consequences hit recruitment and retention

IT workers would risk their job to do what’s right

Data access concerns outweigh possible productivity gains

Conclusion

Methodological Notes
As leaders turn to technology to monitor workforce productivity, they fail to consider the harm they will do to the team responsible for implementation — their IT department.

To understand what happens to IT teams when given such an assignment, 1E surveyed 500 IT workers and 500 IT managers, in partnership with Wakefield Research. The results demonstrate the need for companies to reevaluate using employee productivity surveillance technology (EPST).

Though most IT staff currently work for companies that use EPST, they harbor discomfort about deploying it to watch their colleagues, especially if the company isn’t fully transparent about the practice. Many IT workers report they would raise their concerns with leadership before following orders to deploy this tech, and some would even flat-out refuse. Most IT managers admit they wouldn’t force a staff member to deploy and monitor the tech if they refused. And once EPST is deployed, many in IT say they would defy company policy and inform colleagues about it, even helping them use anti-surveillance workarounds.
Definition

Employee productivity surveillance technology (EPST) refers to a range of tools that companies use to monitor employees’ productivity.

Common EPST

- Monitoring web activity
- Logging time spent using various programs
- Keylogging, click-logging
- Video recording
- Audio recording

“Most research and reporting on this issue to date has focused on the employees that companies spy on. They’re more anxious and resentful, more likely to fake work, quit, and even steal workplace property. Yet, until now, the research has overlooked the perspective of those tasked with spying: IT workers and managers.”

Ian Greenleigh
Vice President of Brand and Communications, 1E
2023 EPST SURVEY

Key Findings

Discomfort abounds

80% of IT managers think staff would be comfortable deploying EPST

46% of IT workers are comfortable deploying EPST

73% of IT managers are uncomfortable telling their staff to deploy EPST

70% of IT Managers wouldn’t force staff to deploy and monitor EPST if they refused
Transparency essential, but lacking

89% 95%

transparency would increase my comfort with my company using EPST

48% of IT managers at companies using EPST say the company didn’t inform employees of its use and/or how it was being done
Leaders, beware

84% 87%

have seen negative impacts since their company started using EPST

48%
of IT workers would turn down an otherwise desirable IT position if they knew the company used EPST
Leaders are concerned about their ability to supervise, especially in remote and hybrid environments — and companies have turned to tech for help. In fact, nearly 9 in 10 IT managers (89%) have first-hand experience with EPST, with 83% saying their current employer uses it and 19% reporting experience with it at a previous company. Similarly, more than 4 in 5 IT workers (84%) describe themselves as very or extremely familiar with EPST, with the same percentage (84%) having first-hand experience with it at a current (77%) or former (21%) employer.

If IT team members don’t already have experience with EPST, they likely will soon. Among IT managers at companies that don’t use EPST today, 4 in 5 (79%*) believe their company is at least somewhat likely to start in the next three years.
83% of IT managers say their current employer uses EPST.

79% of IT managers believe their company is likely to start using EPST in the next 3 years.
More than two-thirds of IT workers (69%) and IT managers (67%) believe it’s appropriate for companies to monitor what employees are really doing on company time. But 31% of IT workers and 33% of IT managers say EPST is an invasion of privacy and shouldn’t be used under any circumstances.

Despite a majority believing it’s an acceptable practice, nearly 3 in 4 IT managers (73%) wouldn’t be comfortable instructing their own staff to deploy EPST. This discomfort serves IT leaders well. Not only do IT workers find the prospect of spying on co-workers unsettling, IT managers also severely underestimate the turmoil this would cause their team. While 4 in 5 IT managers (80%) say their staff would be comfortable with being told to deploy EPST, only 46% of IT workers say they’d be comfortable doing so.

Further, nearly half of IT workers (46%) say requiring them to deploy EPST to monitor their colleagues would cause them even greater anxiety than having their own productivity monitored.
31% of IT Workers and 33% of IT Managers think EPST is an invasion of privacy and should not be used under any circumstances.
Disclosure has a massive impact on the comfort level of IT teams. Nearly all IT managers (95%) and 89% of IT workers say transparency would increase their comfort with their company using EPST. Yet surprisingly, many aren’t seeing that level of transparency in action. Of the IT managers whose current company uses EPST, nearly half (48%) say employees either weren’t informed that the technology is being used at all or were told it is being used but not how the surveillance is being conducted.
89% of IT workers say transparency would increase their comfort with their company using EPST.

95% of IT managers say employees either weren't informed that the tech is being used and/or of how the surveillance is being conducted.

48% of IT managers say employees either weren't informed that the tech is being used and/or of how the surveillance is being conducted.
Before rolling out EPST, company leaders can expect to encounter IT’s unease and should be prepared for a rocky implementation. More than a quarter of IT workers (27%) and a third of IT managers (33%) would raise their concerns with leadership before following an order to deploy EPST and monitor their colleagues.

Some aren’t even willing to raise the issue of a potential compromise. Nearly 1 in 10 IT managers (8%) and 5% of IT workers would outright refuse to deploy the tech.

Fortunately for non-management level staff, those who refuse would have their supervisors’ support: 70% of IT managers wouldn’t force their staff to follow through. Included in that total is a quarter (25%) who would respect staffers’ values and assign the task to others, without even issuing so much as a written warning.
27% of IT workers and 33% of IT managers would raise concerns about EPST with leadership.

70% of IT managers wouldn’t force their staff to follow through.
Using EPST will hamper talent management, affecting both recruitment and retention efforts. If surveilling employees’ productivity becomes part of a company’s brand, it sets them back in the competition for talent. More than half of IT workers (52%) would turn down an otherwise desirable IT position if they knew the company used EPST.

Bringing surveillance tech on board can also spur current employees to seek other opportunities. Three-quarters of IT workers whose company isn’t currently using EPST (75%) say requiring them to deploy the tech to track other employees would negatively impact their willingness to remain in their current position. This includes 30% who would begin actively applying for other positions and 3% who would quit immediately. More than 2 in 5 say it would leave them more open to other offers (41%), making them an easy target for recruiters seeking to fill their IT positions.
have seen negative impacts since company started using EPST
Employees losing trust in company leaders

Employee loyalty declining

Employees quitting

More difficult to hire new staff

Morale declining

Employees burning out faster

Worker anxiety increasing

**Negative impacts** seen at companies using EPST

- IT Workers
- IT Managers
This avoidable talent drain is equally as likely to extend to management. 76%* of IT managers whose company isn’t currently using EPST say having to ask their team to deploy it would negatively impact their willingness to remain in their current position, including more than a third (35%*) who would begin actively applying for other jobs.

The danger radiates to other teams, too. 87% of IT managers and 84% of IT workers at companies using EPST have seen negative impacts since their company started using it. Specifically, respondents say it has led to declining employee loyalty (33% of IT managers and 29% of IT workers) and employees losing trust in company leaders (26% of IT managers and 29% of IT workers).

These IT teams also report impacts to workers’ wellbeing, including increases in worker anxiety (29% of IT managers and 30% of IT workers), quicker employee burnout (29% of IT managers and 28% of IT workers), and declining morale (27% of IT managers and 26% of IT workers).

When a company experiences an increase in distrust and anxiety among workers, elevated employee turnover follows. More than a quarter of IT managers (28%) and IT workers (27%) at companies using EPST have seen employees quit as a result. Exacerbating the situation, nearly as many IT managers (27%) and even more IT workers (30%) say it has become increasingly difficult to hire new staff since the company deployed the tech.

Companies not already using EPST risk a fortune if they choose to spy. As it stands, the potential negative impact is staggering. Nearly half of IT workers (48%) would expect employees to lose trust in company leaders if the company deployed the tech, 42% would expect a decline in employee loyalty, 40% predict employees would quit, and 31% believe it would become difficult to hire new staff.
IT workers would risk their job to do what’s right

Transparency is so important for IT workers that many are willing to sidestep company policy to make sure their colleagues are informed. Nearly 3 in 4 IT workers (73%) would tell other employees the company was using EPST, even if doing so was against policy. Additionally, nearly as many IT workers (72%) would tell colleagues of any known workarounds.

Comfort varies greatly according to the specific surveillance technology used, making it vital that companies are open with employees about their practices. IT professionals are largely aligned in accepting the business case for keeping tabs on productivity, but their sentiment also clearly highlights boundaries. They’re most comfortable with their company monitoring basic online behavior such as web activity (58% of IT workers and 58% of IT managers) and logging time spent using various programs (57% of IT workers and 49% of IT managers).

However, they are more likely to see some proxy measures for productivity as overreach—an invasion of privacy that also has little business value. Less than half are comfortable with their company using keylogging and click-logging (49% of IT workers and 42% of IT managers) or video recording (43% of IT workers and 39% of IT managers). And even fewer are comfortable with screenshot captures (39% of both groups) or audio recordings (36% of IT workers and 39% of IT managers).
of IT workers would tell employees company was using EPST

73%

of IT workers would tell of any workarounds

72%
2023 EPST SURVEY

Data access concerns outweigh possible productivity gains

Though they’ve seen—or would expect—downsides to using EPST, most IT workers (69%) and IT managers (71%) believe worker productivity increases when they know they are being watched.

A quarter of IT workers (25%) and nearly a quarter of IT managers (24%) say the technology’s ability to measure productivity is inaccurate because it doesn’t provide a full view of an employee’s work and contributions.

Less than a third of IT workers (32%) and IT managers (32%) feel an employee’s direct line supervisor should have access to personally identifiable information (PII) collected using the tech. Less than half of IT workers (44%) and IT managers (48%) think senior-level leaders like C-suite or division heads should have access to such PII, either.

Instead, nearly 9 in 10 IT workers (88%) agree employees should have access to their own data, reiterating the importance of transparency.

As IT professionals are responsible for safeguarding data, it stands to reason they believe they’re trained and qualified in its handling: More than 2 in 3 IT workers (69%) and more than 3 in 4 IT managers (76%) feel IT staff should have access to PII collected using EPST.
“It’s very likely that the perceived increase in productivity is actually an increase in ‘presenteeism.’ Other studies have shown that surveilled employees are more than two times more likely to pretend to be working, and spend an average of 67 minutes per day beyond their normal work hours so others see they are online. Acting productive and being productive are very different.”

Ian Greenleigh
Vice President of Brand and Communications, 1E
Conclusion

EPST is becoming extremely common, and the vast majority of those that don’t currently use it are likely to do soon. But IT managers and their staff are uncomfortable spying on colleagues, and many would only do so after speaking up. Among the concerns are the negative impacts on their own well-being and that of employees, doubts regarding the accuracy of the data produced, the creation of talent management problems, and an erosion of trust in leadership and loyalty to the company.

Internal backlash could doom implementation from the start, as the vast majority of IT personnel would disclose its use to colleagues and offer workarounds even if it violated company policy. With nearly half of IT managers who have been at their companies for 5 years or less viewing the technology as an invasion of privacy, the pushback appears likely to continue.

IT departments are now in a precarious position, and companies must decide whether the known risks of using productivity surveillance technology are worth the potential rewards.

*Small base size; findings are directional.*
2023 EPST SURVEY

Methodological Notes

The 1E IT Workers and 1E IT Managers Surveys were conducted by Wakefield Research among 500 US IT workers, employed full-time in non-management roles, at companies of 500 or more employees, and among 500 US IT Managers, with a minimum seniority of manager, at companies of 500 or more employees, between February 16th and February 27th, 2023, using an email invitation and online surveys.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.4 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.
What if each digital employee experience (DEX) was better than the last? The 1E platform helps IT teams improve end user experience, tighten security, reduce costs, and evolve operations from cost center to strategic enabler. Over one-third of the Fortune 100 rely on 1E’s single-agent solution with real-time automation and remediation for more visibility, control, compliance, and observability. Now, all operations teams can provide exceptional employee experiences, increase IT efficiency, and reduce service delivery time.

About 1E

1E.com

About Wakefield Research

Wakefield Research is a leading, independent provider of quantitative, qualitative, and hybrid market research and market intelligence. Wakefield Research supports the world’s most prominent brands and agencies, including 50 of the Fortune 100, in 90 countries. Our work is regularly featured in media.

WakefieldResearch.com