WHITE HOUSE TASK FORCE TO ADDRESS ONLINE HARASSMENT AND ABUSE

FINAL REPORT AND BLUEPRINT

THE WHITE HOUSE
WASHINGTON

Table of Contents

"There will be many policy issues we disagree on…but bipartisan proposals to protect our privacy and our children; to prevent discrimination, sexual exploitation, and cyberstalking; and to tackle anticompetitive conduct shouldn't separate us. Let's unite behind our shared values."

President Joe Biden, Wall Street Journal *Op-Ed, January 11, 2023*

"No one should have to endure abuse just because they are attempting to participate in society…. And all people deserve to use the Internet free from fear."

Vice President Kamala Harris at the launch of the White House Task Force to Address Online Harassment and Abuse, June 16, 2022

Executive Summary

Online harassment and abuse are increasingly widespread in today's digitally connected world. This can include online threats and intimidation as well as various forms of technology-facilitated gender-based violence (TFGBV), such as the non-consensual distribution of intimate images, including non-consensual intimate imagery generated with artificial intelligence (AI) tools, cyberstalking, and sextortion. Women, girls, and LGBTQI+ individuals, particularly those who face intersectional discrimination and bias on the basis of race and ethnicity, gender, religion, disability, sexual orientation, and other factors, are disproportionately affected.

To tackle this scourge, on June 16, 2022, President Biden issued a Presidential Memorandum establishing the White House Task Force to Address Online Harassment and Abuse (Task Force), with a mandate to build a comprehensive approach for how the federal government prevents and addresses gender-based online harms. Since then, the Biden-Harris Administration has taken significant action across 12 federal departments and agencies to prevent and address online harassment and abuse, both domestically and globally.

This includes a record investment of more than $36 million to support survivors through newly established victim services, helplines, and training and capacity-building for individuals and organizations—from law enforcement officials to victim advocates—to enhance their response to TFGBV. Through the Task Force, federal departments and agencies have accelerated prevention, awareness and outreach efforts in communities across the country to promote safe and respectful online interactions, enhance digital literacy, and address online misogyny and cyberbullying as risk factors for offline violence. Federal law enforcement agencies have promoted accountability for perpetrators of cybercrimes that disproportionately impact women and girls, children, and LGBTQI+ people, as well as for technology platforms on which these crimes are often committed. Furthermore, our work to address online harassment and abuse has continued to evolve and respond to new and emerging technology and its impact on survivors, including the rise of generative AI.

The Administration has, for example:

- **Bolstered support to survivors**, including by launching the country's first national, 24/7 Image Abuse Helpline and Safety Center, and implementing the Safe Connections Act of 2022, which the President signed into law to make it easier for survivors of domestic violence to leave a wireless or phone plan shared with an abuser.
- **Strengthened protections for students** who have experienced sexual harassment, including online harassment and abuse, by issuing a new Title IX final rule that clarifies schools' responsibilities under federal law to address sex discrimination and harassment whether the conduct takes place online, in person, or both; and strengthens definitions for sex-based harassment and stalking under Title IX to address the growth in TFGBV, including AI-generated abuse. These protections underscore the need for schools to address online sex-based harassment with the same level of seriousness and responsibility as in-person forms of harassment—a needed shift in our culture to recognize the significant harms associated with TFGBV.
- **Published new guidance for ending and preventing workplace harassment**, **including online harassment and abuse**, by updating the Equal Employment Opportunity

Commission (EEOC) Enforcement Guidance on Harassment in the Workplace. The guidance clarifies employers' responsibilities under federal law with respect to unlawful workplace harassment—including whether the conduct takes place online, in-person, or both—based on sex, race, and other protected characteristics. The guidance also highlights the need for employers to address online sex-based harassment that contributes to a hostile work environment, including the non-consensual distribution of intimate images.

- **Confronted the role of social media in the youth mental health crisis, including exposure to online harassment and abuse,** with the Surgeon General issuing an historic Advisory on Social Media and Youth Mental Health to address the unique safety and privacy risks posed by online harassment and abuse, and highlight its disproportionate toll on the wellbeing of adolescent girls, particularly girls of color and LGBTQI+ youth. Complementing the Surgeon General's Advisory, the Administration has launched the Kids Online Health and Safety Task Force.
- **Championed online safety as a core element of digital equity,** encouraging state leaders charged with implementing more than $50 million in funding through the Digital Equity Act of 2021 to integrate online harassment and abuse prevention strategies into their activities, and prioritizing online safety in the State Digital Equity Capacity Grant Program and the Digital Equity Competitive Grants Program.
- **Invested in efforts to disrupt online pathways to violent extremism by addressing online harassment and abuse**, including through research and community-based programs supported by the Department of Homeland Security to assess behavioral indicators for violent extremism linked to gender-based violence, and tackle risk factors associated with misogynistic threats and online violence.
- **Taken steps to address the risks posed by deepfake image-based abuse** through the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, which: (i) directs the National Institute of Standards for Technology (NIST) to seek input from companies, civil society, and other stakeholders to identify best practices for safeguarding AI systems from generating abuse material; (ii) urges the Office of Management and Budget (OMB) to recommend testing and safeguards against the generation of non-consensual intimate images or child sexual abuse material by government-procured AI models; (iii) tasks OMB with issuing guidance for federal departments and agencies on the use of tools to detect synthetic content and label authentic government-produced content to set an example for the private sector and encourage the global implementation of these safeguards; and (iv) launched the National AI Talent Surge, through which the Biden-Harris Administration is committed to hiring at least 100 AI and AI-enabling professionals with both technical expertise and experience addressing AI-generated harms, including deepfake image-based abuse. These actions build on the principles first established in the Blueprint for an AI Bill of Rights.
- **Elevated TFGBV in our foreign policy and national security efforts** by founding and co-leading the 14-country Global Partnership for Action on Gender-Based Online Harassment and Abuse, through which the Administration has advanced global policies to address online safety for women, girls, and LGBTQI+ persons by issuing joint statements and by tackling online harms through the G7, G20, UN, and other fora, such as through the Christchurch Call to Action, which has newly integrated a focus on gender-based hate and its links with online radicalization and mobilization to violence. The Administration has

also invested at least $15 million in targeted funding to prevent and respond to TFGBV and counter its chilling effects on women leaders and democratic participation as part of our emphasis on supporting democracies globally, including through new initiatives to provide support to women leaders who have experienced extreme threats or forms of online violence. Complementing this work, the Administration has also advanced a comprehensive approach to addressing the proliferation and misuse of commercial spyware, which disproportionately affects women, through for example new export controls, sanctions, and visa restrictions.

A full accounting of completed and ongoing actions based on stakeholder recommendations are detailed in the Task Force Final Report and Blueprint. This Final Report builds on the work from departments and agencies laid out in an initial Blueprint, which was highlighted in its Executive Summary in March 2023.

Introduction

Online harassment and abuse—which encompass a range of harms facilitated by technology—is increasingly widespread in today's digitally connected world. Many forms of online harassment and abuse, such as the non-consensual distribution of intimate images and cyberstalking, disproportionately affect women, girls, and LGBTQI+ individuals, particularly those who face intersectional discrimination and bias on the basis of race and ethnicity, gender, religion, disability, sexual orientation, and other factors.[1] Survivors of online harassment and abuse—especially image-based sexual abuse—are often forced to relive their trauma and face ongoing harms that increase exponentially over time, owing to the viral flow of information on digital media and the difficulty of removing harmful content. Simply put: the design and function of the internet amplify and intensify the scale and spread of gender-based violence (GBV), and platforms have created new modalities for harm.

Online harassment and abuse can severely affect health, disrupt education, and derail careers. Victims and survivors can experience devastating consequences on their mental health, including post-traumatic stress disorder (PTSD), depression, anxiety, eating disorders, self-harm, and suicide, as well as increased risk of physical and sexual violence. Victims and survivors often self-censor and withdraw from online spaces and from broader engagement in the workplace, social settings, political participation, educational opportunities, and the broader economy. The Biden-Harris Administration has also paid particular attention to children's online health, safety, and privacy, including the persistent proliferation of child sexual abuse material traded online, and the growing threat of sextortion, which has increasingly targeted adolescent boys.

Furthermore, as generative AI technology becomes more accessible to the general public, the nonconsensual sharing, dissemination, and monetization of synthetic and altered sexualized images and videos have increasingly been used to perpetuate online harassment and abuse.[2] Non-consensual deepfake intimate images and videos are often used to sexualize, humiliate, and degrade survivors, a disproportionate number of whom are women and children. Even when AI-generated intimate images do not depict a real person, racial, ethnic, and gender biases embedded in models' training data have been demonstrated to perpetuate racist, sexist stereotypes, such as images that depict Asian women as hypersexualized and submissive, reinforcing harmful gender and social norms that contribute to risk for sexual violence online and offline.[3] Further, research has demonstrated that in some cases, AI models have been trained on known child sexual abuse

[1] As defined in the Presidential Memorandum to Establish the Task Force, "technology-facilitated GBV" is any form of gender-based violence, including harassment and abuse, which takes place through, or is aided by, the use of digital technologies and devices.

[2] According to Professor Danielle Citron, there are more than 9,500 sites dedicated to the sharing and distribution of both authentic and deepfake or synthetic NCII—including of adolescent girls—and a growing number of these sites have monetized the generation of deepfake images on-demand, with some sites charging a monthly subscription fee. Danielle Keats Citron "The Continued (In)visibility of Cyber Gender Abuse," Yale Law Journal 133 (2023), https://www.yalelawjournal.org/forum/the-continued-invisibility-of-cyber-gender-abuse.

[3] Melissa Heikkila, "How it feels to be sexually objectified by an AI," *MIT Technology Review*, December 13, 2022, https://www.technologyreview.com/2022/12/13/1064810/how-it-feels-to-be-sexually-objectified-by-an-ai; and Nitasha Tiku, Kevin Schaul, and Szu Yu Chen, "This is how AI image generators see the world," *Washington Post*, 2023, https://www.washingtonpost.com/technology/interactive/2023/ai-generated-images-bias-racism-sexism-stereotypes.

material (CSAM).[4] In addition, generative AI tools can be used to create harassing messages, amplify hate speech, and facilitate doxing—including to undermine women political and public figures, who may decide to leave their jobs or stop speaking out online as a result.

While public awareness of these disturbing trends is improving—in no small part due to the advocacy of survivors—more work remains to address the impacts of online harassment and abuse on individuals and to society at-large. The stakes couldn't be higher: in addition to the devastating effects on individuals, the proliferation of online harassment, abuse and misogyny normalizes this abusive behavior and compromises our democracy and public safety, silencing diverse voices, and facilitating gender-motivated, extremist acts of violence.

To tackle this scourge, in June 2022, President Biden issued a Presidential Memorandum establishing the White House Task Force to Address Online Harassment and Abuse (Task Force), with a mandate to pursue concrete actions across four broad lines of effort: prevention; survivor support; accountability; and research.

The Task Force Final Report and Blueprint present completed and ongoing actions from federal departments and agencies to prevent and address TFGBV.

[4] Thiel, D. "Investigation Finds AI Image Generation Models Trained on Child Abuse." Stanford Cyber Policy Center, December 2023, https://cyber.fsi.stanford.edu/news/investigation-finds-ai-image-generation-models-trained-child-abuse.

Key Findings

Since its launch, the Task Force has heard from hundreds of stakeholders—survivors, advocates, parents, educators, law enforcement, medical and legal professionals, and researchers—who shared the significant harms of online harassment and abuse. These include powerful survivor testimonies from a diverse constituency of youth, college students, public figures, and social media influencers across race and ethnicity, gender, religion, disability, sexual orientation, and gender identity demonstrating the widespread reach of TFGBV. The Task Force spoke with a high school student whose classmates had created and disseminated AI-generated nude images without her consent; a professional athlete whose social media feeds are routinely inundated with racist and sexist threats; a student who was forced to change schools after another student livestreamed her sexual assault; a survivor whose ex-partner doxed, stalked, and harassed him through a dating site; a parent whose daughter's brutal rape and murder by a dating partner were livestreamed; a local elected official who reduced her social media presence and questioned her decision to run for office due to the volume of online threats to her and to her children; a journalist covering democratic elections in her home country who faced foreign-government backed threats, intimidation, and image-based abuse intended to silence her reporting; and a survivor who lost her employment as she coped with depression, PTSD, and severe anxiety stemming from online sexual exploitation she experienced as a child.[5] Survivors also shared their experiences facing major barriers when seeking assistance or support from law enforcement, their schools, colleagues and peers, the courts, or from the technology platforms that had been weaponized for harm.

After hearing extensively from survivors, advocates, and other stakeholders, the Task Force noted common themes:

- **The design and function of online platforms amplify and intensify the scale and spread of GBV.**[6] Survivors of online harassment and abuse—especially image-based abuse—are often forced to relive their trauma and face ongoing harms that increase dramatically over time, owing to the viral flow of information on digital media, the mob effect of others intentionally exacerbating the harm, and the difficulty of removing harmful, non-consensual content from the internet.
- **The rapid rise of generative AI has intensified the already dire problem of NCII sharing and child sexual abuse material (CSAM).**[7] Generative AI tools enable individuals to generate photorealistic NCII or CSAM using the actual faces of individuals

5 All examples shared with the express permission of those depicted, and with personally identifying information excluded.

6 See, e.g., Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review, 107 (2019), https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security.

7 Danielle Keats Citron "The Continued (In)visibility of Cyber Gender Abuse," Yale Law Journal 133 (2023), https://www.yalelawjournal.org/forum/the-continued-invisibility-of-cyber-gender-abuse. In addition, new research from Graphika affirms that "the creation and dissemination of synthetic NCII has moved from a custom service available on niche internet forums to an automated and scaled online business" with the volume in referral link traffic for these services increasing by more than 2000% on platforms such as Reddit in 2023. Santiago Lakatos, A Revealing Picture: AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business (New York: Graphika, 2013), https://public-assets.graphika.com/reports/graphika-report-a-revealing-picture.pdf.

with relatively little technical skills. Moreover, even when synthetic NCII or CSAM does not depict a real person, the training data used to generate these images may include the likeness of actual individuals repurposed without their consent. Regardless of an image's authenticity, survivors experience severe tolls to their mental and physical health and the scale at which these images can be generated is enormous.[8]

- **Online harassment and abuse can be a deliberate tactic used by government and non-government actors to silence women political and public figures, with implications for democracies globally.[9]** Women, girls, and LGBTQI+ political and public figures, peacebuilders, human rights defenders, activists, and journalists are disproportionately targeted by TFGBV, which can impede their meaningful participation in political, public, and economic life. State and non-state actors, including extremist groups and individuals, are increasingly and deliberately engaging in online harassment and abuse, including gendered disinformation and hate speech, to silence leaders and suppress democratic movements.[10] This dimension of online harassment and abuse can be particularly pronounced for women and LGBTQI+ public figures,[11] and is diminishing the ambitions of young people—especially girls—from pursuing careers in politics and other public-facing careers.[12]
- **Online harassment and abuse undermine freedom of expression and participation in everyday life by chilling victims' speech and discouraging help-seeking.** Survivors self-censor and withdraw from online spaces and from broader engagement in academic, workplace or social settings.[13] Friends, family, and well-meaning bystanders who intervene to help can also become the target of sustained harassment campaigns, retaliatory

8 One study found that a group of 34 synthetic NCII providers received over 24 million unique visitors to their websites in September 2023. Lakatos, A Revealing Picture. AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business (New York: Graphika, 2013), https://public-assets.graphika.com/reports/graphika-report-a-revealing-picture.pdf.

9 U.S. Department of State, "Gendered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors," U.S. Department of State Global Engagement Center, March 27, 2023, https://www.state.gov/gendered-disinformation-tactics-themes-and-trends-by-foreign-malign-actors.

10 U.S. Department of State, "2023 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse," Office of the Spokesperson, March 28, 2023; U.S. Department of State, "Gendered Disinformation," https://www.state.gov/gendered-disinformation-tactics-themes-and-trends-by-foreign-malign-actors.

11 For example, a project by researchers at Princeton University examined threats and harassment to local elections, health, and education officials, counting incidents across 43 states, found that women officials were targeted at a higher frequency than others, 3.4x more than men. Joel Day, Aleena Khan, and Michael Loadenthal, *Threats and Harassment Against Local Official Dataset* (Princeton: Bridging Divides Initiative, 2022), https://bridgingdivides.princeton.edu/sites/g/files/toruqf246/files/documents/Threats%20and%20Harassment%20Report.pdf.

12 Plan International, *The Truth Gap: How Misinformation and Disinformation Online Affect the Lives, Learning, and Leadership Girls and Young Women* (Woking, 2021), https://plan-international.org/uploads/2022/02/sotwgr2021-commsreport-en.pdf.

13 For example, in the United States, four in ten young women say they have self-censored to avoid harassment online. Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney, *Online Harassment, Abuse, and Digital Cyberstalking in America* (New York: Data & Society Research Institute, 2016), https://datasociety.net/wp-content/uploads/2016/11/Online_Harassment_2016.pdf; Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab, "Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment" (ACM Conference on Computer Supported Cooperative Work and Social Computing, Portland, 2017), 1231–1245.

"cybermobs" organized by perpetrators, and trolls to silence and intimidate anyone who tries to help.[14]

- **Online harassment and abuse can lead to serious short and long-term harms to victims and survivors' health and wellbeing.** GBV that originates or takes place through technology cannot be dismissed as "just online" or minimized as "not real violence." Victims can experience real, devastating consequences to their mental and physical health, including PTSD, depression, anxiety, eating disorders, self-harm, and suicide.[15] Moreover, a significant proportion of online harassment and abuse involves the sharing, dissemination,[16] and monetization[17] of videos and images of physical acts of sexual violence, exploitation, and abuse (e.g., CSAM,[18] livestreaming rape videos, femicide, and other forms of GBV). Harassment and abuse that happens online can also lead to violence offline, including for women in public life. Addressing this form of GBV requires additional training and specialized services beyond the standard victim services provided for survivors of intimate partner violence, sexual assault, or stalking.
- **As digital technology has become essential to our everyday lives, online harassment and abuse has become pervasive and widespread, risking its normalization, particularly among young people.[19]** Despite increased evidence of its consequences to mental and physical wellbeing, online harassment and abuse has yet to be fully integrated across policies, programs, and approaches to address GBV across the U.S. and globally. While many adults and service providers are insufficiently aware of its harms and impacts, online violence has become so frequent that many young people are starting to see it as normal.[20] Prevention and public awareness efforts at local, state, national, and global levels

---

[14] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Cambridge: Harvard University Press, 2016), 116-118.

[15] Francesca Stevens, Jason R.C. Nurse, and Budi Arief, "Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review," *Cyberpsychology, Behavior, and Social Networking* 24, no. 6 (2021): 367-376, doi: 10.1089/cyber.2020.0253; "Toxic Twitter: The Psychological Harms of Violence and Abuse Against Women Online," Amnesty International, March 20, 2018, https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-6-6; Josh Campbell and Jason Kravarik, "A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases," *CNN*, May 23, 2022, https://www.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html.

[16] At least one in ten young women have been threatened with the public posting of their nude or intimate images. Amanda Lenhart, Michele Ybarra, and Myeshia Price-Feeney, *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of 'Revenge Porn'* (New York: Data and Society Research Institute, 2016), https://datasociety.net/wp-content/uploads/2016/12/Nonconsensual_Image_Sharing_2016.pdf.

[17] Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (New York: WW Norton and Company, 2022), 180-184.

[18] An estimated 16% of young adults have experienced at least one type of sexual abuse online before the age of 18, with girls (23%) and transgender or gender fluid children (20%) disproportionately impacted. David Finkelhor, Heather Turner, and Deirdre Colburn, "Prevalence of Online Sexual Offenses Against Children in the US," *JAMA Network Open* 5, no. 10 (2022), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2797339.

[19] For example, 85% of women note that they have experienced or witnessed some form of online abuse. Group, T. E. (2021, March 3). The Economist Group. Retrieved from https://www.economistgroup.com/group-news/economist-impact/85-of-women-have-witnessed-harassment-and-online-violence-finds-new-research.

[20] In a survey by Plan International, more than half of girls from around the world have been harassed and abused online, and one in four girls abused online feels physically unsafe as a result. Plan International, *Free to be Online? Girls' and young women's experiences of online harassment* (Woking, 2020), https://plan-international.org/uploads/2022/02/sotwgr2020-commsreport-en-2.pdf.

"And after the massacre of 19 children — 19 babies — and 2 teachers in Uvalde, it was revealed that the shooter had threatened to kidnap, rape, and kill teenage girls on Instagram. One of the girls he harassed described the abuse, I quote, as 'just how online is.'" Remarks by Vice President Harris Announcing the Launch of the White House Task

are urgently needed to educate and train law enforcement, parents, teachers, and other systems professionals, while also building digital citizenship skills and fostering norms of respect, safety, privacy, and consent.

Force to Address Online Harassment and Abuse. Silvia Foster-Fau, Cat Zakrzewski, Naomi Nix, and Drew Harwell, "Before massacre, Uvalde gunman frequently threatened teen girls online," *Washington Post*, May 28, 2022, https://www.washingtonpost.com/technology/2022/05/28/uvalde-texas-gunman-online-threats.

Lines of Effort

The final Blueprint of the White House Task Force to Address Online Harassment has led to a broad range of new, ongoing and expanded commitments from Federal agencies to address TFGBV, highlighted in an Appendix. Actions are based on the following lines of effort:

1. **Prevention**, including actions to create healthier online environments for youth and adults, incorporate digital safety curricula into our schools, and provide resources and trainings for parents and educators;
2. **Survivor support**, including efforts to increase training and technical assistance to law enforcement, prosecutors, educators, mental health professionals, and victim advocates, so that survivors can access support and assistance from professionals who recognize the complexities and seriousness of TFGBV;
3. **Accountability**, including improved coordination among Federal, state, Tribal, territorial and local law enforcement agencies to investigate and prosecute sextortion, child sexual exploitation online, the non-consensual distribution of intimate images of adults, and cyberstalking, as well as support for state legislators advancing or strengthening legislation to address image-based abuse, sextortion, and other emerging forms of TFGBV; and
4. **Research**, to inform evidence-based interventions, deepen our understanding of the mental health impacts of youth exposure to online harassment and abuse, and guide upstream efforts to discourage and prevent young men and boys, in particular, from engaging in targeted acts of violence that share roots with online misogyny and other forms of hate.

The Way Forward

When President Biden first wrote and championed the Violence Against Women Act (VAWA) in the early 1990s, the internet was in its infancy. Today, digital technologies have transformed our ability to connect, communicate, and access services and support. At the same time, online platforms and other digital tools are frequently misused as tools of abuse, harassment, and exploitation. As technology evolves, so, too, must our approach to addressing gender-based violence. Through the Violence Against Women Act Reauthorization Act of 2022 (VAWA 2022), which President Biden signed into law in March 2022, the Biden-Harris Administration is taking unprecedented steps to address TFGBV. VAWA 2022 strengthens this landmark, bipartisan law, updating it to reflect the ways in which digital technologies facilitate gender-based violence by:

- Defining technological abuse;[21]
- Establishing a federal civil cause of action for individuals whose intimate visual images are disclosed without their consent, allowing a victim to recover damages and legal fees;
- Creating a new National Resource Center on Cybercrimes Against Individuals; and
- Supporting State, Tribal, and local government efforts to prevent and prosecute cybercrimes against individuals, including cyberstalking and the nonconsensual distribution of intimate images.

The Department of Justice (DOJ) Office on Violence Against Women recently announced $7 million in federal funding opportunities to implement the Local Law Enforcement Grants for Enforcement of Cybercrimes and to launch the National Resource Center on Cybercrimes Against Individuals. DOJ is also holding those who violate the law accountable through groundbreaking federal hate crime prosecutions, including the prosecution and sentencing of a self-identified "incel" or "involuntary celibate," a member of a predominantly male online community that harbors anger towards women, fueled by their inability to convince women to engage in sexual activity with them.[22] And earlier this year, DOJ brought charges against an individual who was sentenced to seven years in prison for the possession of child sexual abuse material depicting sexual violence against young girls, including images and videos generated using AI tools.[23]

The Biden-Harris Administration remains committed to mobilizing federal resources and working with survivors, stakeholders, Congress, industry leaders, and others to prevent, address, and respond to online harassment and abuse. Building on this Blueprint, we will continue to pursue

[21] Section 40002 of VAWA (34 USC 12291) defines technological abuse as "an act or pattern of behavior that occurs within domestic violence, sexual assault, dating violence or stalking that is intended to harm, threaten, intimidate, control, stalk, harass, impersonate, exploit, extort, or monitor, except as otherwise permitted by law, another person, that occurs using any form of technology, including but not limited to: internet enabled devices, online spaces and platforms, computers, mobile devices, cameras and imaging programs, apps, location tracking devices, or communication technologies, or any other emerging technologies."

[22] U.S. Attorney's Office, Southern District of Ohio, "Highland County man sentenced to more than 6 years in prison for attempting hate crime," Press Release, February 29, 2024, https://www.justice.gov/usao-sdoh/pr/highland-county-man-sentenced-more-6-years-prison-attempting-hate-crime.

[23] U.S. Attorney's Office, Eastern District of Virginia, "Fairfax Man Sentenced for Downloading Child Sexual Abuse Videos and Images, Including Computer-Generated Material," Press Release, February 9, 2024, https://www.justice.gov/usao-edva/pr/fairfax-man-sentenced-downloading-child-sexual-abuse-videos-and-images-including.

executive actions to address online safety, health, privacy, and accountability by improving prevention efforts, increasing support for survivors, strengthening accountability for perpetrators and platforms, and deepening the evidence base to inform policy and programs.

Examples of additional actions the Administration is working towards include:

- Launching a new initiative to increase resources and advance women's political participation and leadership in the digital age, including through programs that address online threats to women leaders—a priority of the 2023 Strategy and National Action Plan on Women, Peace, and Security, which recognizes that online violence against women in political and public life is a threat to security and stability;
- Facilitating research partnerships to promote data access for experts studying TFGBV, building on Joint Principles on Combatting Gender-Based Violence in the Digital Environment, which the U.S. and European Union released at the 6th Ministerial of the U.S.-EU Trade and Technology Council;
- Working with close allies and partners to tackle the rise in online child sexual exploitation, including through the Australia-United States Joint Council on Combatting Online Child Sexual Exploitation and France's Children's Online Protection Lab; and,
- Advancing global norms and standards for responsible and trustworthy AI that account for the disproportionate impacts of AI-generated harms on women and girls, including through the newly-launched AI Safety Institute.[24]

Federal and State Laws and Regulations

As the President has underscored, online safety is a bipartisan issue.[25] The President has called for Democrats and Republicans to unite on legislation to hold technology companies accountable, raising the alarm that social media and other platforms have allowed abusive and even criminal conduct like cyberstalking, child sexual exploitation, and non-consensual intimate images to proliferate on their sites.

The Administration will continue to work toward bipartisan legislation to set baseline requirements for users' online safety and privacy, just as consumer protection laws have set standards for products that Americans rely on every day. Federal laws to promote victims and survivors' safety should:

- **Remove special legal protections for large technology platforms.** The President has long called for fundamental reforms to Section 230 of the Communications Act of 1934 (47 U.S.C. 230, enacted as part of the "Communications Decency Act of 1996"). Congress

[24] NIST has identified initial workstreams for the AI Safety Institute, including Working Group #2 on Synthetic Content. The Working Group aims to identify the existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for authenticating content and tracking its provenance; labeling synthetic content, such as using watermarking; detecting synthetic content; and preventing generative AI from producing child sexual abuse material or producing NCII of real individuals; testing software used for the above purposes; and auditing and maintaining synthetic content. Available at U.S. Artificial Intelligence Safety Institute, "AISIC Working Groups," National Institute of Standards and Technology, February 8, 2024, https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute/aisic-working-groups.

[25] The bipartisan nature of this issue was highlighted in the January 2024 Senate Judiciary Committee hearing on "Big Tech and the Online Child Sexual Exploitation Crisis."

should remove special legal protections for online platforms that broadly shields them from liability when they host or disseminate illegal, violent conduct, such as posting someone's address online without their consent paired with rape or death threats (a severe form of doxing). Doing so would bolster safety for survivors of gender-based violence by incentivizing platforms to enforce their terms of service and community standards of conduct.

- **Set transparency requirements for online platforms**, particularly regarding design choices that impact child safety, including publicly accessible information about their algorithmic recommendation systems, content moderation decisions, and enforcement of community standards.
- **Require platforms to enable timely and robust public interest research on the amplification and proliferation of online harassment and abuse**, balancing access to platform data with maintaining users' privacy and other rights.
- **Strengthen legal protections for survivors and victims of non-consensual intimate imagery,** including AI-generated NCII, building on the federal civil cause of action for NCII established under VAWA 2022, as legal experts and advocates have underscored the need to recognize NCII as a serious offense, given the significant harms it causes.

In addition, Congress should provide critical resources for tackling online harassment and abuse by fully appropriating core federal programs that equip communities to prevent and address online harms, including by:

- Fully appropriating the $10 million authorized in Title XIV, Cybercrimes Enforcement, in VAWA 2022 for the Local Law Enforcement Grants for Enforcement of Cybercrimes Program,[26] and fully appropriating the $4 million also authorized in VAWA 2022 for the National Resource Center on Cybercrimes Against Individuals.[27]
- Fully appropriating the $120 million authorized under the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Our Children Act of 2008), which provides critical tools for state and local law enforcement agencies to investigate and prosecute online child sexual exploitation and abuse—a crime that has significantly increased with the rise in generative AI.[28]

State governments also have a role to play in passing laws to promote online safety and privacy. In April 2023, the Task Force convened a group of state legislators at the White House for a discussion on bipartisan legislative approaches to addressing non-consensually distributed intimate images. Since the launch of the Task Force, state governments have been working in parallel to increase accountability for online harms and protect survivors, introducing at least 56 bills and passing an estimated 17 laws aimed at preventing and addressing multiple forms of online harassment and abuse, including state laws creating new civil causes of action for doxing and non-consensually distributed deepfake intimate images.[29]

---

[26] 34 U.S.C. 30107(c).
[27] 34 U.S.C. 30108(i).
[28] Note: Then-Senator Biden was a champion of this legislation in 2008; the President's FY 2024 budget called for full funding at $120 million.
See Drew Harvell, "AI-Generated Child Sex Images Spawn New Nightmare for the Web," *Washington Post*, June 19, 2023, https://www.washingtonpost.com/technology/2023/06/19/artificial-intelligence-child-sex-abuse-images.
[29] See Appendix B: Table of State Legislature Bills and Laws.

★ ★ ★ ★ ★ ★

Actions from Industry

It will take coordinated actions and commitments from all sectors to comprehensively prevent and address online harassment and abuse. Technology companies play a critical role in shaping user experiences, with implications for the health, safety, and privacy of their consumers based on choices they make in the design and operation of their products. Trust and safety experts, working with survivors, parents, researchers and advocates, have identified a number of best practices to strengthen protections and privacy for survivors of online harassment and abuse, which some platforms have adopted in recent years. For example:

- Online platforms—particularly those known to be used by children—can disable direct messaging from unknown accounts, as well as employ image-blurring technology so that users only view images they consent to receive;
- Online platforms can sign on to join initiatives that enable survivors of image-based sexual abuse to securely upload an intimate image or video—including deepfakes—to generate a digital fingerprint of the non-consensual content for removal from participating sites;
- AI developers and online platforms hosting AI-generated content can support watermarking and other technical approaches to labeling AI-generated content;
- Technology companies can invest in trust and safety teams, prioritizing human reviewers to enforce community guidelines and Terms of Service;
- Online platforms can create and maintain accessible, responsive reporting channels for users to flag abusive, threatening or violent conduct; and,
- Online platforms can expand access to public online platform data in a privacy-preserving way and use this data to better understand TFGBV.

Further, with the exponential rise in image-based sexual abuse linked with the rapid advancement of generative AI, we must address the growth in online sites that monetize non-consensual intimate images, and will work with the spectrum of actors who can help to remedy this problem, from payment processors, to mobile app stores and developers, cloud providers, search engines, and more.

Conclusion

Moving forward, the Biden-Harris Administration will continue to prioritize addressing online harassment and abuse as an urgent problem that cuts across domestic and foreign policy, given the borderless nature of digital economies and communities. In addition to working across government to tackle this challenge, we will engage with a broad range of stakeholders to address the ecosystem that enables and, in many ways, normalizes online harms. As work continues, this Task Force will submit a follow-up report to the President on an annual basis. Moving forward, actions by departments and agencies in support of the Task Force will be integrated in to the implementation of the National Plan to End Gender-Based Violence, which the White House released in May 2023 and highlights "online safety" as one of its strategic pillars, including priorities to expand research and data collection and improve services and access to justice for survivors of online harassment and abuse.

Appendix A: Final Blueprint—Completed and Ongoing Actions

Line of Effort 1: Prevention

Youth Education, Digital Literacy, & Engaging Young Men & Boys

- In October 2023, the U.S. Department of Health and Human Services (HHS), through the Administration for Children and Families (ACF), awarded $1.9 million through the Human Trafficking Youth Prevention Education (HTYPE) Program to four local education agencies to partner with expert non-profit organizations and build school-wide capacity to identify and address student's risk for human trafficking in their communities, including prevention education on technology-facilitated human trafficking.
- The Department of Commerce has committed to promoting efforts to prevent online harassment and abuse of children and youth, including through increased awareness of services and support for youth victims of online harassment and abuse through funding made available by the Digital Equity Act of 2021. Between August 2022 and May 2023, the National Telecommunications and Information Administration (NTIA) awarded $53.7M in funding to 56 States and Territories through the State Digital Equity Planning Grant Program, and has encouraged state broadband administrators and other state digital equity leaders to pursue ways of preventing online harassment and abuse, particularly impacting children and youth, as they craft their digital equity plans.
- The Kids Online Health & Safety Task Force is developing voluntary guidance, policy considerations, and a toolkit on safety-, health- and privacy-by-design for industry developing digital products and services to be finalized later this year. To inform these efforts, in October 2023, NTIA issued a request for public comment[30] on the state of industry efforts and technology and the risks to minors, and subsequently received more than 500 comments from parents, kids, industry, academia, advocacy organizations, health and safety experts, and governments.
- In March 2024, NTIA announced the Notice of Funding Opportunity for the Fiscal Year (FY) 2024 State Digital Equity Capacity Grant Program, which will provide $1.44 billion to fund digital literacy projects that can also address online safety and the prevention of online harassment and abuse. NTIA will also conduct stakeholder outreach webinars to facilitate partnerships between administrators of digital equity grants, state domestic violence and sexual assault coalitions, and domestic and sexual violence training and technical assistance providers to promote digital equity and prevent and address online harassment and abuse.
- The Department of Education (ED) has developed promising practices and materials for students, parents, and educators, including curated resources for K-12 educators about online safety, how to respond and report critical online incidents in school settings, and information

[30] In framing these issues, the NTIA request for comment stated: "Safety is also an area of concern related to use of online platforms, particularly the risk of predators targeting minors online for physical, psychological, and other forms of abuse, including sexual exploitation, extortion (or sextortion) and cyberbullying."

on digital rights and responsibilities of students and educators, including online learning. Highlights include:

  - ED's National Center on Safe and Supportive Learning Environments (NCSSLE) has hosted numerous webinars to help K12 educators and other stakeholders prevent and respond to GBV and online harassment and abuse to enhance coverage of online harassment and abuse for educators and other stakeholders in K12 school settings. Some examples include: Human Trafficking Webinar Series - Protecting Young People from Online Exploitation (Oct. 26, 2022); Engaging the Secondary School Community to Prevent GBV (Nov. 2022); Promoting Whole Student Health Through Safe Digital Habits (Nov. 8, 2023). These and many others can be accessed here.
  - In January 2024, ED's Office of Elementary and Secondary Education (OESE) Office of Safe and Supportive Schools launched an online resource page through its Readiness and Emergency Management for Schools (REMS) technical assistance center. The page hosts federal resources focused on Digital Health, Safety, and Security, including online harassment.

- ED will issue resources, model policies and voluntary best practices for school districts on the use of internet-enabled devices (both personal and school-provided) and services in elementary and secondary schools in order to promote and encourage local policies that improve digital health, prevent online harassment and abuse, and promote safety, and citizenship practices and academic outcomes; and the acquisition of safe, healthy, and developmentally-appropriate digital literacy skills and habits for students from preschool to high school (P-12).
- DOJ's Office on Violence Against Women (OVW) prioritized addressing online harm and abuse and TFGBV in their solicitations for FY 2023 and FY 2024 Grants to Prevent and Respond to Domestic Violence, Dating Violence, Sexual Assault, Stalking, and Sex Trafficking Against Children and Youth Program, Grants to Engage Men and Boys as Allies in the Prevention of Violence Against Women and Girls Program, and Grants to Reduce Domestic Violence, Dating Violence, Sexual Assault, and Stalking on Campus Program.
- In January 2024, DOJ's OVW released the FY 2024 Training and Technical Assistance Initiative solicitation, which included a purpose area intended to provide a 24-month grant to improve online safety for children and youth. The award will fund training and technical assistance to children- and youth-serving organizations, schools and school districts, institutions of higher education, and victim service providers to enhance their ability to provide prevention and intervention strategies and responses to children and youth (ages 0 – 24) who have experienced or are impacted by technology-facilitated abuse.
- The Centers for Disease Control and Prevention (CDC) will issue an array of prevention resources aimed at promoting online safety for young people, including: updates to the Community Violence Prevention Resource for Action that summarizes the best available evidence for the prevention of violence among youth and young adults (formerly known as the Youth Violence Prevention Technical Package), including online harassment and abuse, and calls for additional research to build the evidence for online violence prevention; and, updates to the Dating Matters® teen dating violence prevention module to specifically incorporate strategies for the prevention of online harassment and abuse, drawing from CDC's recent evaluation research supporting its effectiveness in addressing multiple forms of youth violence.

★ ★ ★ ★ ★ ★

Tackling Online Misogyny and Preventing Violence[31]

- In FY 2022 and FY 2023, the Department of Homeland Security (DHS) Targeted Violence and Terrorism Prevention (TVTP) Program invested nearly $2 million in projects to support evidence-informed interventions that address online radicalization and its intersections with gender-based hate and online harassment and abuse to programs in 35 states plus the District of Columbia.
- In FY 2023, DHS, through the Federal Emergency Management Agency (FEMA), provided over $6 million through the Non-profit Security Grant Program (NSGP) to non-profit organizations at risk of a terrorist or other extremist attack for cybersecurity measures to assist in preventing, preparing for, protecting against, and responding to acts of terrorism and other threats, including online harassment and abuse, cyberstalking, and misogynistic threats.
- In FY 2023, the DHS Cybersecurity and Infrastructure Security Agency (CISA) conducted dozens of Active Shooter Preparedness Webinars to more than 28,000 registered stakeholders, focused on emergency response and action plans, and covering threatening online behavior, harassment, and abuse, including doxing, and introducing "Pathway to Violence" concepts which identify the expression of misogynistic comments as an evidence-based, behavioral indicator of an individual moving down the pathway to violence, and offering options to prevent incidents of targeted violence.
- In June 2023, DHS led a communications campaign on SchoolSafety.gov focused on the topic of online safety. This effort included stakeholder outreach and accompanying materials to help parents, students, educators, and other members of the K-12 community learn about student online safety and ways to support young people in preventing, recognizing, and responding to online threats, and to disseminate resources available across the Federal government related to online safety.
- ED's OESE, Institute for Education Sciences, and Office of Special Education and Rehabilitative Services have curated a set of resources to support schools that are working to prevent and respond to hate-fueled violence, including gender-based violence, online and offline. ED posted content addressing cyberbullying and online harassment, including gender-based online harassment and abuse, on its Free to Learn/United We Stand website.

Public Awareness and Additional Prevention Efforts

- In December 2022, the Federal Bureau of Investigations (FBI), DHS Homeland Security Investigations (HSI), and National Center for Missing and Exploited Children (NCMEC) issued a national public safety alert highlighting an incremental rise in financial sextortion cases, incidents of children and teens being coerced into sending explicit images online and extorted for money.
- In 2023, HSI also created a dedicated website to provide information to the public on financial sextortion. DHS has increased efforts to build awareness and prevent these crimes by incorporating financial sextortion into its Project iGuardian™ program materials. Project iGuardian™ offers in-person presentations designed to inform children, teens, parents, and

[31] (Consistent with relevant legal authorities, federal policy, and privacy, civil rights, and civil liberties protections).

trusted adults on the threat of online child sexual exploitation and abuse and how to implement preventative strategies and report suspected abuse to law enforcement.

- In January 2024, DHS published an infographic on resources for individuals on the threat of doxing. The infographic defines what doxing is and outlines proactive steps individuals can take to prevent themselves from doxing. The infographic also recommends steps that can be taken to protect individuals who are victims of doxing.
- In April 2024, DHS launched a first-of-its-kind national public awareness campaign, Know2Protect: Together We Can Stop Online Child Exploitation, to counter the rapidly escalating crisis of online child sexual exploitation and abuse (CSEA). The campaign educates children, caregivers, policymakers, and the broader public about the growing threat of online CSEA and how to keep children safe online. Campaign partners include technology companies, national and international sports leagues, youth-serving organizations, non-profits, and law enforcement.
- HHS Office on Trafficking in Persons (OTIP) is integrating the impact of online harassment and abuse and its intersection with human trafficking in new materials developed for prevention and outreach for children and youth under the HHS Look Beneath the Surface public awareness campaign., The campaign will release additional materials that will seek to promote safe online behaviors, including "understanding and recognizing technology-facilitated exploitation and trafficking," "destigmatizing and countering myths," and "increasing trust in seeking help."
- FEMA's Individual and Community Preparedness Division (ICPD), in consultation with Save the Children, launched its Child Safeguarding guidance and training to ensure that all FEMA personnel who work directly with youth to advance preparedness and resilience are taking the appropriate steps to mitigate risk to program beneficiaries. This includes specific recommendations for safely engaging with youth on virtual platforms, including webinars, social media, and video-conferencing, and highlights the protections and steps required to prevent children from receiving direct messages from adult attendees of the FEMA's Youth Preparedness Council's virtual events in order to reduce risk for child sexual exploitation and abuse. In 2023, FEMA completed the development of its training and will work with partners to increase the numbers of training deliveries to other FEMA and DHS employees in 2024.
- In July 2023, USAID launched the Youth Well-Being Prize Competition, which awards young changemakers for ideas on how to protect young people's well-being and safety and make a positive impact on the lives and communities of themselves and their peers. Awardees will be recognized for proposing solutions that tackle digital harm and GBV, including TFGBV. Prizes are expected to be awarded in Summer 2024.
- Since the launch of the Task Force, the U.S. Agency for International Development (USAID) has convened an annual Protecting Children and Youth from Digital Harm Symposium. In February 2024, USAID hosted the 2024 Symposium to identify and tackle digital harm issues and provide an international forum to learn, share, and engage with youth leaders, government, civil society, donors, and the private sector. The Symposium had nearly 1,500 people registered with representation from 126 countries and had over 40 hours of programming that addressed a wide range of issues facing children and youth, including TFGBV.

- In February 2023, ED Secretary Cardona with the Surgeon General and other external stakeholders held an in-person town hall on student mental health. The conversation highlighted the mental health impacts of online harassment and abuse, featuring student voices and mental health experts.
- As part of a DOJ Office for Victims of Crime (OVC) grant, the National Domestic Violence Hotline is partnering with Esperanza United to launch a public awareness campaign on social media focusing on relationship abuse, including online harassment and abuse, launched in April 2024. This awareness effort is designed as Spanish first—meaning content is created to be culturally specific and relevant to the Latina community.
- In March 2024, the U.S. and EU launched recommendations for protecting human rights defenders online, including from gendered online harassment and abuse, through the Trade and Technology Council. The United States built upon these joint recommendations by launching comprehensive guidance that sets out best practices and actions online platforms can take to protect human rights defenders and other activists online.

★ ★ ★ ★ ★ ★

GLOBAL PARTNERSHIP FOR ACTION ON GENDER-BASED ONLINE HARASSMENT AND ABUSE

A commitment from the first Summit for Democracy and launched at the 66th United Nations Commission on the Status of Women, the Global Partnership for Action on Gender-Based Online Harassment and Abuse (Global Partnership), which currently has 14 participating governments, brings together international organizations, civil society, and the private sector to prioritize, understand, prevent, and address the growing scourge of technology-facilitated gender-based violence (TFGBV) through championing policy, investing in programs, and collecting research and data to inform this work.

First, the Global Partnership is driving policy change to set international norms recognizing TFGBV as a threat to democracy and security, in addition to its individual harms. Countries on the Global Partnership, working in coordination with civil society, strengthened language to combat TFGBV across a range of international frameworks and policies, including the G7, G20, UN General Assembly, and more. In addition, the Global Partnership led policy-related statements issued as a part of the Christchurch Call and the Freedom Online Coalition.

As a commitment to joining the Global Partnership, member countries have increased support for domestic, regional, and global programs addressing TFGBV. The U.S. government has invested at least $15 million in targeted foreign assistance programs to combat TFGBV since the Global Partnership's launch and will establish a new Global TFGBV Rapid Response Fund for women politicians, political candidates, and civil society leaders who have experienced extreme forms and/or threats of TFGBV and need urgent access to flexible resources to meet their immediate needs.

The Global Partnership is also expanding data and research on TFGBV. For example, USAID included questions on TFGBV within demographic and health surveys' domestic violence module surveys released in 2023 in three countries, Nigeria, Zambia, and Lesotho. The Global Partnership is also developing a framework for coordinated action to prevent and disrupt the spread of gendered disinformation and democratic rollback in the context of electoral processes, and achieve a common understanding of the range of interventions that can be deployed to disrupt disinformation tactics, hosting a conference on this topic in Nairobi, Kenya in March 2024. The outcomes of this conference will inform the final framework developed.

★ ★ ★ ★ ★ ★

Line of Effort 2: Survivor Support

Victim Services

- Through the FY 2023 grant program to Build Capacity of National Crisis Hotlines, DOJ OVC prioritized online harassment and abuse, awarding $6 million to the following initiatives:
  - In September 2023, DOJ OVC funded the first-ever national helpline for survivors of image-based sexual abuse operated by the Cyber Civil Rights Initiative, which will significantly expand support to survivors of online harassment and abuse and meet the rising need for services related to the non-consensual distribution of intimate images, including sextortion and synthetic intimate images, or "deepfakes."
  - OVC also funded the National Domestic Violence Hotline and the National Center for Victims of Crime (NCVC) to enhance the responsiveness and effectiveness of national hotlines in addressing the needs of survivors of TFGBV. This grant will ensure advocates are trained to recognize multiple forms of TFGBV, supporting survivors with referrals to specialized services, and addressing the impact on marginalized communities. The Hotline will award a portion of these funds to Abused Deaf Women's Advocacy Services to enhance services for survivors experiencing online harassment and abuse in the Deaf/Blind community. NCVC will also increase its VictimConnect Resource Center capacity and accessibility to better support survivors experiencing TFGBV.
- Through OVC's FY 2023 Advancing the Use of Technology to Assist Victims of Crime Solicitation, the University of Wisconsin-Madison is creating a remote tech clinic program to help combat technology-facilitated intimate partner violence and increase access to support for survivors living in remote parts of the state.
- In FY 2023, OVC awarded almost $1 million in additional grant funding to projects providing services for survivors of technology-facilitated intimate partner violence and image-based sexual abuse, including support to the Sanar Institute's Reclaim Project, which will address the traumatic impact of image- based sexual abuse through a combination of direct service and capacity building, training, and education.
- In November 2023, the Federal Communications Commission (FCC) adopted a Report and Order implementing the line separation provisions of the Safe Connections Act of 2022. The new rules will make it easier for survivors to access domestic violence hotlines, leave a family wireless phone plan, and afford phone service.
- HHS OTIP has expanded efforts to prevent and address technology-facilitated human trafficking through the National Human Trafficking Hotline by training hotline call specialists to address technology abuse among trafficking in persons (TIP) victims, and by collecting and reporting on data collected by the Hotline on technology abuse among TIP victims. In FY 2023, there were 9,877 human trafficking situations reported to the Hotline with one or more victim. Of the 4,878 situations where venue of trafficking was reported, there were at least 919 technology-facilitated situations.
- In 2023, HSI received more than 8,529 Cybertip reports related to online financial sextortion of minors, primarily boys, leading HSI to open 923 investigations on financial sextortion, and resulting in the identification and rescue of 561 victims.

- In October 2023, ED's OESE published guidance communicating that addressing gender-based violence and cyberbullying are allowable uses of funds under the Bipartisan Safer Communities Act Stronger Connections Grant program.

Support for Civil Society Organizations Working to Address TFGBV Globally

- In March 2023, USAID and the Bill & Melinda Gates Foundation announced a new fund to accelerate closing the gender digital divide with a combined investment of $60 million, at least half of which will focus on Africa. Addressing safety and security, including TFGBV, is one of the five core areas of focus, and integrating safety and security considerations through risk mitigation and other measures will be expected of all projects. Additionally, it's expected that many of the projects will have addressing TFGBV as one of their core objectives.
    - Complementing this effort, the Biden-Harris Administration launched the Women in the Digital Economy Initiative, a public-private partnership with more than $515 million in commitments at its 2023 launch from governments, the private sector, and civil society to accelerate progress to close the gender digital divide and fully integrate women in our globalized, networked economy, including by supporting women's cybersecurity and online safety.
- In March 2023, USAID launched Transform Digital Spaces (Transform), an initiative of up to $6 million over three years that supports pilot projects by women-led civil society organizations to address TFGBV, women's political and civic participation, and digital democracy across Guatemala, Kenya, and Georgia.
- In 2023, USAID launched the Advancing Women's and Girls' Civic and Political Leadership Initiative, working to address individual, structural, and sociocultural barriers to women's civic and political leadership, including violence against women in politics and public life, in both its online and offline manifestations. To date, the initiative is focused on nine initial countries: Côte d'Ivoire, Kenya, Nigeria, Tanzania, Colombia, Ecuador, Honduras, Kyrgyz Republic, and Yemen. For example, initiative-supported activities in Côte d'Ivoire in the lead up to the 2023 local and regional elections included partnering with a local organization to monitor and report on incidents of online violence against women candidates. The findings of this monitoring exercise will inform future work to prevent and mitigate this harm.
    - Since announcing the Advancing Women's and Girls' Civic and Political Leadership Initiative at the first Summit for Democracy, USAID has allocated over $15 million in nine focus countries to build and sustain women's participation in political and civic engagement, including actions to address online violence against women in political and civic life. USAID will provide up to $10 million in additional FY23 funding to support women leaders experiencing violence in-person, as well as threats facilitated by technology, subject to availability of funds.
- In September 2023, the Department of State Bureau of Democracy, Human Rights, and Labor (DRL) supported two programs in Africa and the Western Hemisphere implementing survivor-centered initiatives to prevent and address TFGBV.
- USAID launched the Donor Principles for Human Rights in the Digital Age (Principles) at the Internet Governance Forum in October 2023 in Kyoto, in partnership with the International

Development Research Centre. The Principles call on donors to enhance the safety and security of our partners and the communities they serve, including by addressing technology-facilitated GBV and increasing representation of women, girls and LGBTQI+ persons across all parts of countries' digital ecosystems. So far, 38 governments have endorsed the Principles, and they have broad support from civil society and the private sector.

- In November 2023, the Department of State's Secretary's Office of Global Women's Issues (GWI) announced Supporting Her Empowerment: Leading Engagement and Digital Safety to Stop TFGBV (SHE LEADS), a $3 million project to prevent, mitigate, and respond to TFGBV in South and Central Asia.
- In January 2024, the Department of State announced a solicitation for proposals to support a new Global TFGBV Rapid/Emergency Response Fund. This Department of State-led initiative will provide $2 million for rapid/emergency response support to women politicians, political candidates, and civil society leaders who have experienced extreme forms or threats of TFGBV globally.
- In March 2024, State launched a new $1.975 million program, "Safe Online: Empowering Women in the Digital Economy," to address risks of technology-facilitated gender-based violence facing women in business and the obstacles to women's inclusion in the digital economy in the Caucasus. In partnership with local organizations in each country, the program will encourage governments and private companies to implement online gender-based violence and sexual harassment policies to improve the environment for women in business. This program is supported by the Gender Equity and Equality Action Fund.
- Department of State DRL is piloting a multi-year regional program in Fiji and Indonesia focused on prevention and documentation of TFGBV with $750,000 awarded in September 2022 and, pending availability funds, will continue to be funded in 2024 with an additional $500,000.
- The Department of Commerce has committed to incorporating online harassment and abuse prevention and response strategies into programs designed to help women leverage online tools and technologies to start and grow businesses, such as the Women Accessing Global E-Commerce Initiative (WAGE), which will address enabling environment challenges and market entry barriers that women-owned business may face when conducting cross-border e-commerce. For example:
    - In August 2023, the Department of Commerce and State GWI hosted a workshop at APEC for women entrepreneurs, technology companies, and policymakers on promoting women's entrepreneurship in e-commerce, which included strategies to prevent online harassment and abuse.
    - Through WAGE, the Department of Commerce will continue work within APEC to raise awareness of online harassment and abuse and promote prevention strategies. The next engagement will be a workshop for women entrepreneurs engaged in e-commerce to be held in May 2024 in Peru.

Training and Technical Assistance

- HHS OTIP has integrated online harassment and abuse into existing training and technical assistance to trafficking victim advocates through OTIP grant programs and contracts,

including: an Information Memo to community-based service providers on addressing online harassment and abuse in tech-facilitated human trafficking in July 2022; listening sessions with experts and survivor leaders in August 2022 and November 2023; and through topical presentations at the National Human Trafficking Prevention Summit in August 2023.

- Through support from HHS's Office of Family Violence Prevention and Services (OFVPS), the National Domestic Violence Hotline developed specialized training in partnership with DOJ OVC on TFGBV and trained all 150 victim advocates who answer calls on behalf of the Hotline in December 2023, expanding their capacity to engage in safety planning and make referrals for services to address tech-enabled domestic violence. Specialized training on TFGBV was also integrated into all new advocate training.
- HHS OFVPS has integrated online harassment and abuse into existing training and technical assistance to domestic violence victim advocates provided through OFVPS grant programs, including: Promising Futures, a project of Futures Without Violence that raises awareness around teen dating violence with a particular focus on digital abuse; and the National LGBTQ Institute on Intimate Partner Violence, which developed new training materials for advocates that incorporate the unique and specific ways that LGBTQI+ intimate partner violence (IPV) survivors experience online harassment and abuse.
- In Spring 2024, OVW released solicitations for two new federal opportunities authorized in VAWA 2022, including:
    - the FY 2024 National Resource Center on Cybercrimes Against Individuals solicitation, which will support a cooperative agreement for $2 million to establish and maintain a national resource center that will provide information, training, and technical assistance to improve the capacity of individuals, organizations, governmental entities, and communities to prevent, enforce, and prosecute cybercrimes against individuals (defined as the use of electronic interactive devices to harass, threaten, stalk, extort, coerce, cause fear to, or intimidate an individual, or without consent distribute intimate images of an adult); and
    - the FY 2024 Local Law Enforcement Grants for the Enforcement of Cybercrimes Against Individuals Program Solicitation, which will support training for law enforcement, prosecutors, and judicial personnel, educating the public on cybercrimes against individuals, supporting victim assistants, establishing task forces, and acquiring computers and equipment necessary to conduct investigations and forensic analysis of evidence. OVW expects to make up to ten awards for an estimated $5,000,000.
- OVW's FY 2024 Training and Technical Assistance Initiative solicitation includes a purpose area for $250,000 for a 24-month award to provide training and technical assistance to children and youth-serving organizations, schools and school districts, institutions of higher education, and victim service providers to enhance their ability to provide prevention and intervention strategies and responses to children and youth (ages 0 – 24) who have experienced or are impacted by technology-facilitated abuse.
- As part of a DOJ OVC 2023 Building Capacity of National Crisis Hotlines grant, the National Center for Victims of Crime, the lead facilitator of the National Hotline Consortium (a group of leading national victim services and crisis intervention hotlines), will engage in a collaborative needs assessment of survivors of online abuse and harassment by conducting a series of listening sessions in the coming months. Data collected from the listening sessions,

including narratives, insights, and recommendations from survivors, will form the basis of a public-facing comprehensive report that will include a summary of results and actionable recommendations for national hotlines to better respond to the identified needs of survivors of online harassment and abuse.

- ED has incorporated attention to online harassment and abuse in grant documents indicating that funds can be used, and are encouraged to be used, for these purposes, as appropriate to the specific grant. For example:
    - State and local educational agencies can use Student Support and Academic Enrichment (SSAE) grant funds under Title IV, Part A of the Elementary and Secondary Education Act of 1965 (ESEA) to address bullying and harassment, including online harassment and abuse. As further described in program FAQs: "funds can be used to reduce incidences of bullying and harassment against all students, including bullying and harassment based on a student's (or their associates) actual or perceived race, color, national origin, sex (including gender identity), disability, sexual orientation, religion, or any other distinguishing characteristics that may be identified by the state or [local educational agency]." In addition, local educational agencies that receive SSAE funds and use them for computers and internet access are subject to the internet safety requirements in section 4121 of the ESEA (20 U.S.C. 7131).

★ ★ ★ ★ ★ ★

EXECUTIVE ORDER ON SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE

The Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence directed actions for the U.S. Department of Commerce and the Office of Management and Budget (OMB) to safeguard the use of AI with regard to image-based sexual abuse in several key ways:

- **Promoting industry best practices for addressing the risks and harms of synthetic content.** The Executive Order directs the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce to undertake an initiative for evaluating and auditing capabilities relating to AI technologies through a report which covers issues including means to authenticate content, ways to measure and evaluate the quality of AI-generated synthetic content, and tools to assess and prevent the dissemination and harm from synthetic child sexual abuse material and non-consensual intimate imagery.

- **Leading by example through federal policies.** The Executive Order instructs OMB to issue guidance to agencies for labeling and authenticating official government digital government. OMB has also issued a Request for Information (RFI) to help inform its development of an initial means to ensure the responsible procurement of AI in government, including to reduce the risk that an AI system or service agencies acquire may produce harmful or illegal content, such as fraudulent or deceptive content, or content that includes child sex abuse material or non-consensual intimate imagery.

- **Hiring an AI workforce with trust and safety expertise.** The Executive Order also created the AI and Tech Talent Force to scale up hiring across the federal government for AI talent on key projects. The Office of Personnel Management has granted flexible hiring authorities for federal agencies to hire AI talent, including through government-wide tech talent programs. Recruiting top AI talent—professionals with both technical expertise and experience addressing AI-generated harms, including deepfake image-based abuse—equips the federal government with the expertise needed to better understand and respond to the risks and opportunities of this emerging technology.

★ ★ ★ ★ ★ ★

Line of Effort 3: Accountability

Holding Perpetrators Accountable through the Justice System

- Between Summer 2023 and Spring 2024, the HSI-led "Operation Renewed Hope" has led to the positive identification or rescue of over 175 victims of child sexual exploitation and abuse. This number continues to increase regularly as leads are being investigated by HSI and partner law enforcement agencies.
- Through the work of the DHS Council on Combating Gender-Based Violence, DHS issued a new Management Instruction, a statement that ensures technology-facilitated gender-based crimes may be qualifying criminal activities for U nonimmigrant status (U visa), depending on the facts of each case. The Instruction was finalized on November 6, 2023.
- Under the FY 2023 Training and Technical Assistance Initiative solicitation, DOJ OVW made a 36-month award for $1,000,000 to Aequitas for the Prosecution and Investigation of Online Abuse Initiative, which supports the provision of training and technical assistance to law enforcement and prosecution agencies to enhance their capacity to investigate and prosecute online crimes such as cyberstalking, online harassment, doxing, and threats to share or sharing of intimate images.
- In June 2023, DOJ issued the 2023 National Strategy for Child Exploitation, Prevention, and Interdiction, highlighting the evolving and shocking growth in the online threat to children and emphasizing the efforts, goals, and proposed solutions to stop child sexual exploitation, hold offenders accountable, and protect victims. The Strategy fulfills the statutory requirements of the PROTECT Our Children Act of 2008, and reflects the totality of the federal government's work across federal investigations prosecutions, grants, policy and research initiatives, and other efforts to prevent and address child exploitation offenses.
- DOJ is working to implement the Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018 (AVAA). The AVAA established the Child Pornography Victims Reserve (Reserve) to provide a set amount of monetary assistance to eligible individuals who are depicted in child sexual abuse material that serve as the basis for certain convictions. DOJ published a notice of proposed rulemaking on June 5, 2023 and aims to publish a final rule in June 2024.
- DHS and DOJ will work with the National Center for Missing and Exploited Children (NCMEC) to create combined image repositories used to identify victims, as well as detect and investigate offenses involving CSAM. This work will complement the efforts by NCMEC to empower young people with a tool to help remove or stop the sharing of private images or videos taken of them before the age of 18, through the Take It Down platform.
- In March 2024, the Department of State updated multiple pages on travel.state.gov to deter individuals convicted of child sexual exploitation and abuse, including online, from unlawfully traveling overseas through the addition of clear instructions outlining legal requirements for individuals to self-identify as sex offenders in their applications for a U.S. passport.
- The U.S. Citizenship and Immigration Service (USCIS) will issue a notice of proposed rulemaking that would clarify and update eligibility, procedural, and filing requirements for U nonimmigrant status and adjustment of status for U nonimmigrants. U visas are set aside for

individuals who are victims of certain crimes, including technology-facilitated qualifying criminal activity, and are assisting law enforcement or government officials in the investigation.

- USCIS will also update the U and T Law Enforcement Resource Guides and related online materials to specifically address the intersection between technology facilitated crimes and eligibility for U and T nonimmigrant status.

Workplace Accountability and Agency Capacity-Building

- In October 2022, the Department of Veterans Affairs (VA) issued an update to Veterans Health Administration (VHA) Directive 5019.02, Harassment, Sexual Assaults and Other Defined Public Safety Incidents in VHA, including by adding information regarding the display or recording of intimate images or videos in the definition for sexual harassment, and clarifying that policy on sexual assault reporting and accountability extends to acts that may occur on VA information technology systems. VA is also in the process of updating VA Handbook 5979, Harassment Prevention Program and Procedures, which addresses harassment prevention and response in VA facilities, and will incorporate cyber harassment, including information on how to report various forms of cyber harassment and avenues of redress for victims.
- Since August 2023, the VA Office of Resolution Management, Diversity and Inclusion has hired 12 harassment prevention specialists to add to the current 8 that are charged with developing and overseeing the harassment prevention policy; is providing training and policy guidance to managers, supervisors and employees regarding VA harassment prevention policy implementation and interpretation; and is ensuring harassment prevention policy and reporting procedures are posted throughout facilities and local websites. These prevention specialists will be trained to recognize and respond to cyberbullying and cyber stalking and how to prevent and respond to cyber harassment. Complementing these efforts, in December 2023, VA established resource guide for employees experiencing online harassment and abuse on its VA intranet.
- In December 2022, the Department of Defense (DOD) updated its sexual harassment policies for military personnel to clarify that perpetration does not require physical proximity, and that "the act may be committed through online or other electronic means, including social media and other forms of communication."
- In 2023, USAID created six video modules to train staff working on digital development projects to increase awareness of TFGBV and improve their integration of risk mitigation strategies. The Closing the Gender Digital Divide webpage hosts these videos and additional resources. So far, the trainings have been delivered to USAID staff and implementing partners in Kenya, Nigeria, Ethiopia, and Ghana with ongoing plans for additional trainings in more regions where USAID operates.
- In 2024, USAID published a rule proposing revisions to the Agency for International Development Acquisition Regulation (AIDAR) to incorporate new requirements for Protection from Sexual Exploitation and Abuse (PSEA) and update existing child safeguarding requirements, covering all manners, methods, and mediums of violence, exploitation, and abuse—accounting for new and constantly evolving forms of technological harm. The forthcoming final rule will require USAID-funded contractors to develop survivor-centered prevention and response policies; develop a context-specific compliance plan for large awards;

report incidents immediately and report follow-up actions; and be completely transparent with the Agency and the Office of Inspector General (OIG) from intake through resolution of an incident.

- In April 2023, the Equal Employment Opportunity Commission (EEOC) issued a technical assistance document, Promising Practices for Preventing Harassment in the Federal Sector, which provides practical tips for preventing and addressing harassment within the federal civilian workforce. The document raises awareness about online harassment and abuse in the workplace and highlights promising practices for agencies to address it, such as incorporating information on monitoring for online harassment during management training. The agency has also begun incorporating online harassment and abuse in training for EEOC enforcement staff and external stakeholders.

Enhanced Protections for Students/Accountability for Schools

- In April 2024, ED issued a new Title IX final rule that clarifies schools' responsibilities under federal law to address sex discrimination and harassment whether the conduct takes place online, in person, or both, and strengthens definitions for sex-based harassment and stalking under Title IX to address the growth in TFGBV, including AI-generated abuse.
- In January 2024, ED published a Request for Information (RFI) on Sexual Violence at Educational Institutions on behalf of the interagency Task Force on Sexual Violence in Education to inform future recommendations required by VAWA 2022 for schools to address sexual violence in education. The RFI solicited information on online threats, harassment, and intimidation, and other forms of technological abuse.
- ED's Office for Civil Rights (OCR) has taken action to enforce schools' obligations under Title IX to promote safe learning environments for all students, regardless of sex, including by addressing online incidents of sexual violence, harassment and abuse. Since the launch of the Task Force, for example, OCR has:
    - Resolved investigations involving online threats of sexual violence against girls by other students, which prompted the school district to hold a dress code assembly only for girls, but failed to address the threatening and harassing online behavior by other students. OCR has required the school district to review and revise its dress code to ensure that it does not discriminate on the basis of sex; to train staff regarding their Title IX obligations with respect to responding to reports of sexual harassment and enforcing the dress code; to review and investigate reports of sexual harassment at the high school; and to assess the need for supportive measures for students.
    - Resolved a complaint that arose from the distribution of intimate photos of a high school student taken without consent, followed by reference to their distribution in a school publication that prompted further exposure of the incident, exacerbating a hostile environment for the affected student. OCR has required the school district to provide training to school administrators and teachers on the district's Title IX policies and grievance procedures, and pledged to assess the effectiveness of this training, requiring the district to report back to OCR with documentation of this assessment for review and approval of any needed follow up.

- ED will issue guidance to help institutions comply with section 485(f) of the Higher Education Act of 1965 (commonly known as the "Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act" or the "Clery Act") and educate students and employees about their rights and options under the law. This forthcoming guidance will clarify that certain acts of online harassment and abuse, including the non-consensual distribution of intimate images, are reportable offenses under the Clery Act when they occur as part of a pattern of cyberstalking and for hate crimes that are classified as acts of intimidation.

Promoting Accountability for the Tech Sector and Industry

- The United States and the United Kingdom have jointly tracked progress in the four years since the publication of the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* that were jointly developed by DOJ, DHS, and ministerial counterparts from Australia, Canada, New Zealand, and the United Kingdom in consultation with six technology companies (Facebook, Google, Microsoft, Snap, Twitter, and Roblox), and a broad range of experts from industry, civil society, and academia. Since then, G7 Interior Ministers have added their support, and a total of twenty companies have endorsed the principles. At the Five Country Ministerial in June 2023, the Five Countries implemented a process which requires companies to demonstrate how they adhere to the voluntary principles prior to official endorsement. The Five Countries will look to endorse new criteria for the Voluntary Principles at the 2024 Five Country Ministerial ahead of the Voluntary Principles' five-year anniversary in 2025.
- In May 2023, the Biden-Harris Administration announced the formation of a federal Task Force on Kids Online Health & Safety to promote the health, safety and privacy of minors online by identifying and mitigating the potential adverse health effects of online platforms and formulating recommendations including those for industry. Chaired by HHS and in close partnership with the Department of Commerce, the Task Force is comprised of senior representatives from multiple federal agencies.
- In March 2024, the Administration advanced a comprehensive whole-of-government approach to combatting the misuse of commercial spyware, including to target and intimidate women activists, political figures, and journalists. This has included an Executive Order limiting the U.S. Government's use of commercial spyware from companies that have been linked to human rights abuses globally, a global coalition of countries committed to establishing robust guardrails to prevent the misuse of commercial spyware, and new export controls, visa restrictions, and sanctions against those who misuse or enable the misuse of commercial spyware.
- In January 2024, the FCC sent letters to automakers in response to reporting about how connected cars or "smartphones on wheels" are being weaponized in abusive relationships, noting cars may be "covered providers" under the Safe Connections Act of 2022, which gives the FCC authority to assist survivors of domestic violence and abuse with secure access to communications. The letter requested responses from automakers on connectivity options, including information on connected apps and devices, policies for survivors, privacy and retention policies, and more.
    - In April 2024, the FCC adopted a Further Notice of Proposed Rulemaking that sought to address concerns that survivors may have limited ability to remove an abuser from their vehicle's connected services. In the Further Notice, the Commission seeks

comment on whether changes are needed to its rules implementing the Safe Connections Act to better address the impact of connected car services on domestic violence survivors. The item seeks comments on the types of connected cars available today and on additional actions the Commission can take to assist survivors in accessing safe and affordable connectivity via connected cars.

- In March 2024, NTIA published a report on AI accountability policy, which discusses what kind of data access is necessary to conduct audits and assessments, how regulators and other actors can incentivize and support credible assurance of AI systems along with other forms of accountability, and what different approaches might be needed in different industry sectors, such as employment or health care. This report provides recommendations on whether and how AI systems can be held accountable for facilitating in online harassment and abuse, including the creation and distribution of NCII and CSAM.
- In May 2024, the Department of Commerce announced several draft publications intended to help improve the safety, security and trustworthiness of AI system, which will be published this summer and implement the President's Executive Order on AI, including:
    - Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, which is intended as a companion to the NIST's AI Risk Management Framework, and includes technical recommendations for voluntary use in the design, development, use, and evaluation of AI products, services, and systems, including recommendations for addressing AI-related risks that constitute "Obscene, Degrading, and/or Abusive Content," such as eased production of and access to synthetic CSAM, and NCII of adults; and
    - Reducing Risks Posed by Synthetic Content, which identifies existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, related to synthetic content, including harmful content, such as child sexual abuse material and non-consensual intimate imagery of actual adults. This report will build on NIST's AI Risk Management Framework and enable the development of voluntary guidelines for industry to promote responsible development and testing of AI models to reduce the risk of image-based abuse.

★ ★ ★ ★ ★ ★

PROTECTING CONSUMERS ONLINE THROUGH ENFORCEMENT ACTIONS

In December 2022, the Federal Trade Commission (FTC) settled two actions against Epic Games, Inc., creator of the popular video game Fortnite, requiring the company to pay a total of $520 million in relief. The FTC alleged that Epic Games violated the Children's Online Privacy Protection Act (COPPA) and employed dark patterns (design practices to intentionally manipulate users) to charge consumers without authorization. In a first-of-its-kind provision, the FTC also required Epic Games to adopt strong privacy default settings for children and teens, ensuring that voice and text communications are turned off by default. This requirement is based on the FTC's allegation that children and teens had been bullied, threatened, harassed, and exposed to dangerous and psychologically traumatizing issues such as suicide while communicating with other users on Fortnite.

In January 2024, the FTC settled two actions against firms that operate in the geolocation data marketplace. For years, advocates have voiced concerns about such third-party data brokers and the sale of information to abusers used to stalk, harass, intimidate, and assault, including links to intimate partner homicides.

In the first action, against data broker X-Mode Social, the FTC alleged that that the company unlawfully sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship, and domestic abuse shelters. In a first-of-its-kind provision, the FTC secured a ban that prohibits the company from sharing or selling sensitive location data to third parties.

In the second matter, against data aggregator InMarket Media, the FTC alleged that the company failed to obtain informed consent before collecting and using consumers' location data and unlawfully used consumers' sensitive location information to target them with advertisements. The FTC's settlement includes a ban on the sharing of any precise geolocation data along with a requirement that the company delete or destroy all the location data it previously collected unless it obtains consumer consent. The settlement also prevents the company from using, selling, or otherwise sharing any products or services that categorize or target consumers based on sensitive location data, such as domestic abuse shelters.

★ ★ ★ ★ ★ ★

Line of Effort 4: Research

Federal Surveys and Data Collection

- The CDC updated the National Intimate Partner and Sexual Violence Survey (NISVS), which measures national prevalence of GBV, to include experiences of TFGBV, such as the non-consensual distribution or threat of distribution of intimate images. Data analysis is currently underway with results anticipated for publication by Fall 2024.
- CDC is expanding the Violence Against Children and Youth Surveys, which measure physical, emotional, and sexual violence against children and youth up to age 24 globally, to include measures for technology-facilitated and online violence, and will also field this survey for the first time in the United States. Questions about technology-facilitated and online violence include cyberbullying, online harassment and abuse, and unwanted sexual experiences online. CDC began fielding the survey in Tanzania in Spring 2024 and anticipates publishing the results in Fall 2025.[32]
- In 2023, DOD updated harassment data collection and reporting requirements to include the use of social media and other forms of electronic communication. The data will help DOD identify gaps in policies and ensure a safe and respectable environment for our military and civilian workforces. Beginning in 2023, the following annual reports and prevalence surveys have been updated to include incidents in which social media or other electronic means are used as a means of harassment, discriminatory harassment, and sexual harassment:
    - The Workplace and Equal Opportunity Report
    - The Hazing and Bullying Report
    - Sexual Harassment Assessment Report
    - Military Service Academies Sexual Harassment and Sexual Assault Report
    - Annual Report of Military Equal Opportunity (MEO) Complaints
- DOD will add cyber harassment to the 2024 Armed Forces Workplace and Equal Opportunity Survey, which assesses Service members' attitudes and perceptions about relations in the Military, workplace climate, readiness, well-being, training, and policy effectiveness.
- To better understand the scope, prevalence, scale, and types of TFGBV experienced, in 2023, USAID pre-tested questions on TFGBV within the DHS domestic violence module surveys in Nigeria and Zambia. Based on feedback from pre-testing, TFGBV questions have been included in the DHS for Zambia, Nigeria, and Lesotho with surveys expected to be completed by the end of 2024. This will provide stronger data on TFGBV in these countries and will inform efforts to scale data collection on TFGBV.
- Funded by DOJ OVC, the National Domestic Violence Hotline is updating its data collection terms and methods in order to best capture and report on the real-time experiences of those impacted by tech-facilitated and online abuse and harassment. These updates will expand the

[32] Other Violence Against Children and Youth Surveys have collected questions on technology-facilitated violence, but there is still no internationally standardized classification of these events, which CDC is working to advance, in order to improve data quality and comparability in the same way it has for other forms of injuries and violence.

identification of technology-facilitated abuse and enable better support and future research on the topic.

- ED and the DOJ Bureau of Justice Statistics are developing a survey to implement a requirement under VAWA 2022, which directs the Secretary of Education, in consultation with the Attorney General, to develop a standardized online survey tool regarding postsecondary student experiences with domestic violence, dating violence, sexual assault, sexual harassment, and stalking. The survey will include questions on events related to online sexual harassment, stalking, and abuse.

Research to Understand the Impact of Technology-Facilitated GBV and Inform Evidence-Driven Interventions

- The National Opinion Research Center, through funding from DOJ OVW, collected nationally representative data on technology-facilitated abuse in the United States to assess its scope and nature, as well as determine survivors' access to services and any unmet needs. The project published multiple journal articles in 2023, including on identifying and characterizing technology-facilitated abuse experienced by older adults, sexual and gender minorities, and young adults.
- In December 2023, the National Institutes of Health (NIH) hosted a two-day virtual workshop on "Understanding the Health Impacts of Online Harassment and Abuse" to identify gaps, opportunities, and challenges in advancing a research agenda to better understand the clinical, health, and developmental impacts of online harassment and abuse and develop innovative prevention and intervention efforts. The workshop was informed by a landscape analysis produced by NIH to highlight current projects to expand the evidence base on TFGBV across the life course, a summary of which is available on the NIH Violence Research Initiatives webpage. To further support ongoing research in this area, the NIH Violence Workgroup has established an online harassment and abuse subcommittee to promote coordination and collaboration on research priorities across the NIH and continue to encourage investigator-initiated research in this area.
- The National Domestic Violence Hotline used FVPSA funding to field a survey that asked survivors contacting the Hotline and the Love is Respect Dating Abuse Helpline through digital chat services about their experiences with online harassment and abuse. The Hotline heard from approximately 1,000 survivors who completed the survey, with every respondent reporting they had experienced at least one form of online harassment or abuse, including: 45% who reporting cyberstalking; 27% reporting being threatened with the posting of intimate images without permission; 17% reporting the posting of intimate pictures without permission; and 12% reporting sextortion. These findings will help inform the Hotline's training for victim advocates and referrals to specialized services to ensure people who experience online harassment and abuse are supported in the best ways possible.
- HHS OTIP initiated a study in 2022 that draws on data from King County, Washington as a case example to improve understanding of the risk factors and experiences of individuals who engage in online commercial sexual exploitation of children.
- DOD has initiated two studies to address cyber harassment in response to a recommendation made by the Independent Review Commission to Address Sexual Assault in the Military,

including an estimate of the prevalence of cyber harassment across the force, and review of the effects on online echo chambers on harmful behaviors online.

Research on the Links between Online Misogyny, Extremism, and Targeted Violence

- In January 2023, the U.S. Secret Service's National Threat Assessment Center (NTAC), under DHS, released Mass Attacks in Public Spaces: 2016 – 2020, a comprehensive report examining 173 incidents of targeted violence and highlighting the observable commonalities among the attackers. The report reinforces NTAC's prior research demonstrating that individuals who perpetrate acts of targeted violence frequently display histories of concerning behavior, including hate-based beliefs, domestic violence, harassment, and threatening online communications.
- In March 2023, State's Global Engagement Center published key findings from their report *Gendered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors*. The report found that disinformation often strategically targets women and people with intersecting identities to discourage freedom of expression and undermine democracy.
- Through the Targeted Violence and Terrorism Prevention (TVTP) Program, the DHS Science & Technology (S&T) Directorate issued two grant awards in 2023 to examine GBV, including online threats, as a risk factor for targeted violence.[33] Projects include the development of a risk assessment for targeted violence and terrorism from a public health lens that will integrate threats of online harassment and abuse and gender-based violence as indicators of violence and training for law enforcement and homeland security professionals.
- The DHS Science and Technology Directorate will begin a new study running from July 2024 to July 2026 with the University of Illinois Chicago to research facilitators and barriers for the implementation of school-based assessment teams to identify risk for incidents of violence in schools across Connecticut, Illinois, and Massachusetts. DHS obligated $1M for this study that will develop guidance to promote school safety through enhancing protective factors, and will incorporate links with GBV and online threats.
- In 2023, USAID contributed additional funds to the What Works Phase 2 Program with the Government of the UK's Foreign, Commonwealth & Development Office to contribute to the Sexual Violence Research Initiative's targeted call for proposals on TFGBV to better understand the mental health impacts of online violence targeting women leaders, women with disabilities, indigenous women, and LGBTQI+ women, among others.
- By the end of 2024, CDC expects to publish research that will deepen the evidence base to understand online misogyny as a public health problem by exploring beliefs related to sexism and hate and experiences of online harassment and abuse among adult users of online gaming platforms.
- Through the Global Partnership for Action on Gender-Based Online Harassment and Abuse, the U.S. and UK are developing a response framework for coordinated, evidence-informed action to prevent, disrupt, and reduce the spread of targeted online campaigns against women

[33] Research awards are consistent with relevant legal authorities, federal policy, and privacy, civil rights, and civil liberties protections.

political and public figures and human rights defenders, which will be informed through a first-of-its-kind global conference on countering gendered disinformation held in Kenya March 2024. The framework will be completed by Fall 2024.

★ ★ ★ ★ ★ ★

Appendix B: List of Task Force Roundtables

Launch of the White House Task Force to Address Online Harassment and Abuse

Date: June 16, 2022
Link to Readout

- Sloane Stephens, U.S. Open Tennis Champion, survivor, and mental health advocate
- Matthew Herrick, survivor and advocate
- Francesca Rossi, survivor and victim advocate, Licensed Clinic Social Worker
- Mary Anne Franks, President and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative; Eugene L. and Barbara A. Bernard Professor in Intellectual Property, Technology, and Civil Rights Law, George Washington University Law School
- Carrie Goldberg, Victims' rights attorney at C.A. Goldberg, PLLC
- Melissa Diaz, Chief, San Diego District Attorney/National District Attorneys Association

Roundtable with Victim Advocates and Service Providers

Date: August 22, 2022

- National Domestic Violence Hotline
- EndTAB (End Technology-Enabled Abuse)
- Stalking Prevention, Awareness, and Resource Center (SPARC)
- National Network to End Domestic Violence (NNEDV)
- Cornell Tech Abuse Clinic
- Cyber Civil Rights Initiative (CCRI)

Meteor Collective Roundtable – Online Violence and What It Costs Us

Date: September 14, 2022

- Vital Voices
- Phumzile Van Damme, former Member of Parliament, South Africa
- Hannah Allam, The Washington Post
- International Women's Media Foundation

Roundtable on Engaging Men and Boys in Prevention

Date: October 6, 2022

- Anti-Defamation League (ADL)
- Equimundo Center for Masculinities and Social Justice
- FUTURES Without Violence

- Colorado Sex Offender Management Board
- Professor Jane Stoeyer, University of California, Irvine School of Law
- Eugene Schneeberg, former Office of Faith-Based and Community Partnerships, Obama Administration
- Dr. Saeed Hill, Center for Awareness, Response, and Education (CARE), Northwestern University

Youth Roundtable

Date: October 11, 2022
Link to Readout

- American Academy of Pediatrics Council on Communications and Media
- National Center for Missing & Exploited Children
- School Safety Resource Center in the Colorado Department of Public Safety
- PLAN International
- Love is Respect

Roundtable on Criminal Justice System Responses to Online Harassment and Abuse

Date: November 4, 2022

- Public Safety and Youth Initiatives for the Office Attorney General for the District of Columbia (OAG)
- Homeland Security Investigations
- Aequitas
- American Association for Justice (AAJ)
- Thorn

White House State Legislative Convening on Non-Consensually Distributed Images

Date: April 26, 2023
Link to Readout

- Danielle Citron, Jefferson Scholars Foundation Schenck Distinguished Professor in Law and Caddell and Chapman Professor of Law at University of Virginia; Vice President, Cyber Civil Rights Initiative
- Elisa D'Amico, Owner, eLaw Firm PLLC; Advisor, Cyber Civil Rights Initiative; Co-Founder, Cyber Civil Rights Legal Project
- Courtney J. Fields, speaker and advocate
- Mary Anne Franks, President and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative; Eugene L. and Barbara A. Bernard Professor in Intellectual Property, Technology, and Civil Rights Law, George Washington University Law School

- Lindsey M. Song, Deputy Director, Courtroom Advocates Project, Sanctuary for Families
- Florida State Senate Democratic Leader Lauren Book (D)
- Alabama State Senator Vivian Figures (D)
- Connecticut State Representative Kevin Ryan (D)
- Illinois State Senator Mary Edly-Allen (D)
- Illinois State Representative Jennifer Gong-Gershowitz (D)
- Maryland State Delegate Jon Cardin (D)
- Massachusetts State Representative Michael Day (D)
- Massachusetts State Representative Jeffrey Roy (D)
- Mississippi State Senator Jeremy England (R)
- North Carolina State Representative Diamond Staton-Williams (D)
- Utah State Senator Michael McKell (R)
- Vermont State Representative Barbara Rachelson (D)
- Virginia State Delegate Jackie Glass (D)
- Virginia State Delegate Marcus Simon (D)
- Washington State Representative Tina Orwall (D)

National Domestic Violence Hotline Conference Listening Session on Understanding Online Harassment and Abuse in the Context of Domestic Violence: Strategies for Survivor Support

Date: October 23, 2023

- Courtney J. Fields
- Michelle Gonzalez, Executive Director, Cyber Civil Rights Initiative (CCRI)
- Crystal Justice, Chief External Affairs Officer, National Domestic Violence Hotline
- DOJ Office of Violence Against Women
- DOJ Office for Victims of Crime

Roundtable on AI Safety & Solutions for Image-Based Sexual Abuse

Date: November 13, 2023

- UK Secretary of State for Science, Innovation, and Technology
- #MyImageMyChoice
- Internet Watch Foundation
- Digital Rights Foundation
- Thorn

- Revenge Porn Helpline and StopNCII.org
- National Center for Missing and Exploited Children
- Cyber Civil Rights Initiative
- Association for Progressive Communications
- Dr. Elissa Redmiles, Georgetown University
- Dr. Hany Farid, University of California Berkeley
- Renee Di Resta, Stanford Internet Observatory

Appendix C: Examples of State Laws and Bills Addressing Online Harassment and Abuse[34]

2023				
Bill	**State**	**Year**	**Status**	**Details**
HB 287	AL	2023	Passed	Creates the crime of doxing and establishes criminal penalties.
HB1028	AR	2023	Passed	Replaces the term "child pornography" with child sexual abuse material (CSAM).
AB 1394	CA	2023	Passed	Adds a section defining terms about CSAM hosted on social media platforms on an existing bill related to commercial sexual exploitation.
AB1394	CA	2023	Passed	Requires social media platforms to facilitate reporting of CSAM, and allows judges to assess statutory damages for each instance of CSAM that were aided or abetted by social media platforms.
HB 2123	IL	2023	Passed	Creates a civil case of action against any person who knowingly distributes, creates or solicits a digital forgery of another individual without their consent and for the purpose of harassing, extorting, threatening or causing harm to the falsely depicted individual.
HB 2954	IL	2023	Passed	Allows people a civil private right of action against the individual who doxed them.
HB 3289	IL	2023	Passed	Defines "anxiety" in the statute defining cyberstalking based on the Diagnostic and Statistical Manual definition of anxiety to provide more clarity in the criminal code.
SB 175	LA	2023	Passed	Criminalizes deepfakes involving minors and defines the rights to digital image and likeness.
HB1370	MN	2023	Passed	Creates a cause of action for nonconsensual dissemination of deep fake sexual images, establishes using deep fake technology to influence an election as a crime, and establishes the nonconsensual dissemination of deep fake sexual images as a crime.

[34] Disclaimer: this list is not intended to be exhaustive but is rather illustrative of state legislative activity on online harassment and abuse. Inclusion in this list in no way represents an endorsement by the White House.

SB 660	MO	2023	Passed	Creates a task force examining cyberstalking to make sure that state law is adequately protecting victims.
SB 1517	NJ	2023	Passed	End the "stranger loophole" that makes it more difficult for victims of stalking or cyber harassment to seek protective orders against people they're not related to.
SB 1042	NY	2023	Passed	Includes "deep fake" images within the definition of unlawful dissemination or publication of an intimate image.
SB 2041	ND	2023	Passed	Unauthorized Disclosure of Intimate Images Act - applies the Revenge Porn Act to both adults and children.
SB 1361	TX	2023	Passed	Creates a criminal offense for the unlawful production or distribution of sexually explicit videos using deep fake technology.
SB 5152	WA	2023	Passed	Requires clear disclosure when manipulated or synthetic video, images, and audio are used in election-related media.
HB 1335	WA	2023	Passed	Establishes penalties for the unauthorized publication of personal identifying information.
SB 397	CT	2023	Introduced	Requires social media providers to enforce minimum age requirements and develop content filters for younger users.
HB 1220	HI	2023	Introduced	Prohibits cyber harassment and cyberstalking. Allows for civil liabilities and injunctions for both.
SB 1742	IL	2023	Introduced	Amends the Election code, creates a Class A misdemeanor if the person, with the intent to injure a candidate or influence the results of an election, creates a deep fake video and causes the deep fake to be published or distributed within 30 days of an election.
HB 72	MA	2023	Introduced	Establishes a Massachusetts state deepfake and digital provenance task force to protect against deep fakes used to facilitate criminal or torturous conduct.
SB 1116	MA	2023	Introduced	Establishes the right to freedom from doxing, making it illegal and providing a cause of action for victims.
SB 3707	NJ	2023	Introduced	Incorporates the non-consensual disclosure of sexually deceptive audio or visual media into the state's invasion of privacy statutes. Non-consensual sharing of deepfakes would be a crime of the third degree, punishable by 3-5 years imprisonment, a fine of up to $15,000, or both.

AB 5511	NJ	2023	Introduced	Criminalize the creation of deepfakes that are later used to aid the commission of certain crimes, like extortion or harassment, among others.
AB 5512	NJ	2023	Introduced	Establishes the Deep Fake Technology Unit within the Division of Criminal Justice to assist in the detection and prevention of deceptive audio or visual media.
AB 842	NJ	2023	Introduced	Provides that manipulation of certain caller identification information may constitute cyber-harassment and stalking.
AB 4807	NJ	2022	Introduced	Broadens statute that criminalizes cyber-harassment of a minor.
SB 3926	NJ	2023	Introduced	Extends crime of identity theft to include fraudulent impersonation or false depiction by means of AI or deepfake technology.
AB 5333	NJ	2023	Introduced	Prohibits deepfake pornography and imposes criminal and civil penalties for non-consensual disclosure.
AB 4217	NY	2023	Introduced	Provides for a private right of action for the unlawful dissemination or publication of deep fakes, establishes the crime of aggravated harassment by means of electronic or digital communication.
AB 1202	NY	2023	Introduced	Requires development of an abusive behavior, bullying, and cyberbullying in the workplace prevention training program for all employees.
AB 3112	NY	2023	Introduced	Establishes that a person who knowingly cyberbullies a minor repeatedly is guilty of an unclassified misdemeanor.
SB 79A	NY	2023	Introduced	Establishes the crime of doxing a police officer or state officer with the intent to threaten, intimidate, or incite the commission of a crime of violence against the police officer or their family.
HB 1405	OK	2023	Introduced	Establishes injunctive relief, cumulative remedies, and civil offenses for online harassment.
HB 5698	RI	2023	Introduced	Allows for a civil action against parents of a student who demonstrates willful or wanton disregard for the duty to supervise their child who has committed the offense of cyberstalking or cyberharassment.
SB 1044	TX	2023	Introduced	Creates a criminal offense for the publishing, distribution of deep fake videos 90 days before the date of the election with the intent to deceive and with the

				intent to injure a candidate or influence the results of an election.
HB 1139	WA	2023	Introduced	Establishes penalties for online harassment of elections officials.
HB 4625	TX	2023	Failed	Includes cyberbullying in the definition of bullying in the Education Code, sets forth strategies to prevent or mediate bullying in schools.
HB 1391	VA	2023	Failed	Establishes a Commission on Social Media to study and make recommendations on the impacts and harms to citizens caused by threats, harassment, doxing, misinformation, defamation, etc. occurring on social media.
HB 3058	SC	2023	Failed	Creates the offense of cyber harassment and establishes penalties.
SB 182	GA	2023	Failed	Includes the offense of doxing and penalties for doxing in the stalking section of the Georgia code.
HB 591	FL	2023	Failed	Requires content moderation features from social media apps, and develops regulations by the State Department of Agriculture and Consumer Services
HB 6410	CT	2023	Failed	Creates guidelines that ensure elected officials are accessible to the people they serve while protecting them from abusive, offensive, or threatening online harassment
HB 0139	WY	2023	Failed	Creates a new criminal offense of intimidation of election officials, including doxing them.

2024				
Bill	**State**	**Year**	**Status**	**Details**
SB314	WI	2024	Passed	Revises penalties for child pornography offenses.
AB 664	WI	2024	Passed	Requires disclosure of content generated by AI in political advertisements, providing a penalty.
HB265	AK	2024	Introduced	An act changing the term 'child pornography' to 'child sexual abuse material'.
HB2138	AZ	2024	Introduced	Adds "any computer-generated image" to the state's definition of child exploitation material.
SB217	OH	2024	Introduced	Adds AI-generated images into existing laws criminalizing obscene material of minors.
HB367	OH	2024	Introduced	Penalizes the creation of 'deepfake' material.
HB148	UT	2024	Introduced	Clarifies that prohibited materials depicting sexual exploitation include AI/computer-generated videos/media.
HB238	UT	2024	Introduced	Clarifies that CSAM includes AI-generated media.
HB1143	VA	2024	Introduced	Replaces the term 'child pornography' with CSAM.
AB1831	CA	2024	Introduced	Clarifies that prohibited materials depicting child sexual exploitation include AI/computer-generated videos/media.
HB1545	FL	2024	Introduced	Revises penalties for specified offenses involving children, creating the offense of harmful communications with minors online.
SB1656	FL	2024	Introduced	Revises penalties for specified offenses involving children, including child sexual exploitation.