ASPEN TECH POLICY HUB

POLICY

Technology Safety Initiative Policy Brief

LODRINA CHERNE

EXECUTIVE SUMMARY

The Department of Justice's Office of Violence Against Women (DOJ OVW) should launch a Technology Safety Initiative that provides domestic violence service organizations and their clients a one-stop resource guide to address technology-facilitated abuse and the harms that occur when technology is layered on top of domestic violence and stalking. Domestic violence survivors and their service providers do not currently have a clear place within the federal government to turn to for resources around technical safety. The Office on Violence Against Women has a unique opportunity to use funding from the Emerging Issues in Violence Against Women program in 2022 to lead this initiative to help survivors stay safe online.

As part of the Technology Safety Initiative, OVW should convene experts across domestic violence, stalking, and cybersecurity to evaluate, develop, and provide information for service providers and their clients seeking safety planning, survivors' rights, and resources. DOJ OVW should prioritize technology safety initiatives surrounding nonconsensual device monitoring – including cyberstalking and purpose-built surveillance apps ("stalkerware") – within this initiative to help people who believe they are experiencing nonconsensual cellphone, computer, and account monitoring.

BACKGROUND

Nationwide, up to 37 percent of US adults are estimated to have experienced technology-facilitated abuse.[1] Technology-facilitated abuse can take many forms and includes nonconsensual monitoring of cellphone use, location tracking, or controlling access to devices. The prevalence of technology-facilitated abuse is unfortunately growing; a recent Bureau of Justice Statistics report, for example, notes that survey respondents are more likely to be stalked using technology than through traditional physical stalking.[2]

Victims of technology-facilitated abuse are not sure whom to contact and often must seek help from an array of service providers, including national hotlines, local shelters, local/state/federal law enforcement, lawyers, and friends and family. With a few notable exceptions,[3] local service providers often do not have the expertise to give survivors technical assistance to combat online stalking and nonconsensual device monitoring. As technology-facilitated abuse is often associated with intimate partner violence, there is a dire need to address these harms.[4]

Though multiple Office of Justice Programs (OJP) initiatives address the issue of technology-facilitated abuse, these resources are not scalable nor regularly updated. The Office on Violence Against Women, for example, provides resources about stalking and domestic violence, but doesn't delve into the specifics of technology-facilitated stalking and violence. Many programs address specific aspects of technology-facilitated abuse, but none consider the relationship between civil society organizations and the various government programs. Office for Victims of Crime grantees, including the National Network to End Domestic Violence Technology Safety project, advise survivors of domestic violence on device safety. The National Criminal Justice Reference Service (NCJRS) has provided early research about cyberstalking, and the National Institute of Justice (NIJ) has provided recent guidance and definitions around technology-facilitated abuse.[5] It is challenging for someone new to this topic – whether survivor, technical expert, counselor, or law enforcement agent – to figure out the best way to understand best practices. The disjointed nature of these programs is challenging even before engaging in the nuances that may exist in local jurisdictions.

Moreover, while these offices each provide information about cyberstalking and other technology-facilitated abuse topics, there is no central federal resource guiding organizations that support those experiencing technology-facilitated abuse. The Computer and Internet Crime reporting portal at Justice.gov and the Internet Crime Complaint Center (IC3) are dedicated to harms due to online activity; however, they contain no information about how to manage technology-facilitated abuse and are meant for reporting, not assisting survivors. Because there is no strategic oversight and measurement of the problem, the millions of people experiencing stalking and other forms of harassment via technology will continue to suffer real harms.

RECOMMENDATIONS

OVW should create a Technology Safety Initiative that will:

- Convene experts on domestic violence, stalking, and cybersecurity to evaluate, develop, and identify resources around technology-facilitated abuse; and
- Host a website that will centralize identified resources from the expert convening around preventing and mitigating tech-facilitated abuse.

Using FY2022 Emerging Issues in Violence Against Women program funding, the Technology Safety Initiative would serve as a centralized resource to fight technology-facilitated abuse, addressing an emerging trend in gender-based violence.[6] Capitalizing on expertise within the OVW program around domestic violence and stalking, the Tech Safety Initiative would address two of the most commonly voiced issues in this space: serving as an authoritative government program on technology-facilitated abuse, and symbolizing that the Federal Government acknowledges the harm and severity of the issue.

The ultimate output of this initiative, a website, would serve as a one-stop shop for resources for all types of tech-enabled abuse, including existing OJP resources and those from other organizations across the federal and social service sectors. The first version of this website should be a simple, easy-to-navigate place for service providers and survivors to find resources around existing guidance, statutes, and other material to facilitate safety planning.

The Technology Safety Initiative website should begin by addressing the intersection of technology, domestic violence, and stalking, and should provide information for service providers and survivors about what to do and whom to reach out to. The site should initially focus on topics such as cyberstalking, nonconsensual device monitoring, and stalkerware. As the program matures, additional forms of technology-facilitated abuse such as sextortion, nonconsensual image abuse, doxing, and others (such as those included in a 2020 NIJ-sponsored report on technology-facilitated abuse) should be included.[7]

IMPLEMENTATION

Details on implementing a Technology Safety Initiative and initial website including website requirements, marketing, and budget recommendations are provided in the attached Technology Safety Initiative Operational Plan.

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

THE ASPEN INSTITUTE

1 Amanda R. Witwer et al., *Countering Technology-Facilitated Abuse* (Santa Monica: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RRA108-3.html.

2 Jennifer L. Truman and Rachel E. Morgan, "Stalking Victimization, 2016," US Bureau of Justice Statistics, April 2021, https://bjs.ojp.gov/content/pub/pdf/sv16.pdf.

3 Some organizations that have done a good job of providing survivors technical assistance to combat tech-facilitated abuse include Cornell's Clinic to End Tech Abuse and some state domestic violence coalitions.

4 "Preventing Intimate Partner Violence," US Centers for Disease Control and Prevention, last updated November 2, 2021, https://www.cdc.gov/violenceprevention/intimatepartnerviolence/fastfact.html.

5 "Technology Safety," National Network to End Domestic Violence, accessed February 1, 2022, https://nnedv.org/content/technology-safety/; Randy McCall, "Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada, Concepts and Recommendations," National Criminal Justice Reference Service, May 2004, https://www.ojp.gov/ncjrs/virtual-library/abstracts/online-harassment-and-cyberstalking-victim-access-crisis-referral; "Ranking Needs for Fighting Digital Abuse: Sextortion, Swatting, Doxing, Cyberstalking and Nonconsensual Pornography," National Institute of Justice, November 20, 2020, https://nij.ojp.gov/topics/articles/ranking-needs-fighting-digital-abuse-sextortion-swatting-doxing-cyberstalking.

6 "U.S. Department of Justice FY 2022 Budget Request – Addressing Gender-Based Violence," US Department of Justice, accessed February 1, 2022, https://www.justice.gov/jmd/page/file/1398856/download.

7 *See* National Institute of Justice, *supra* note 5.

ASPEN TECH
POLICY HUB

TECHNOLOGY
SAFETY INITIATIVE

THE ASPEN INSTITUTE