ASPEN TECH POLICY HUB

Technology Safety Initiative Operational Plan

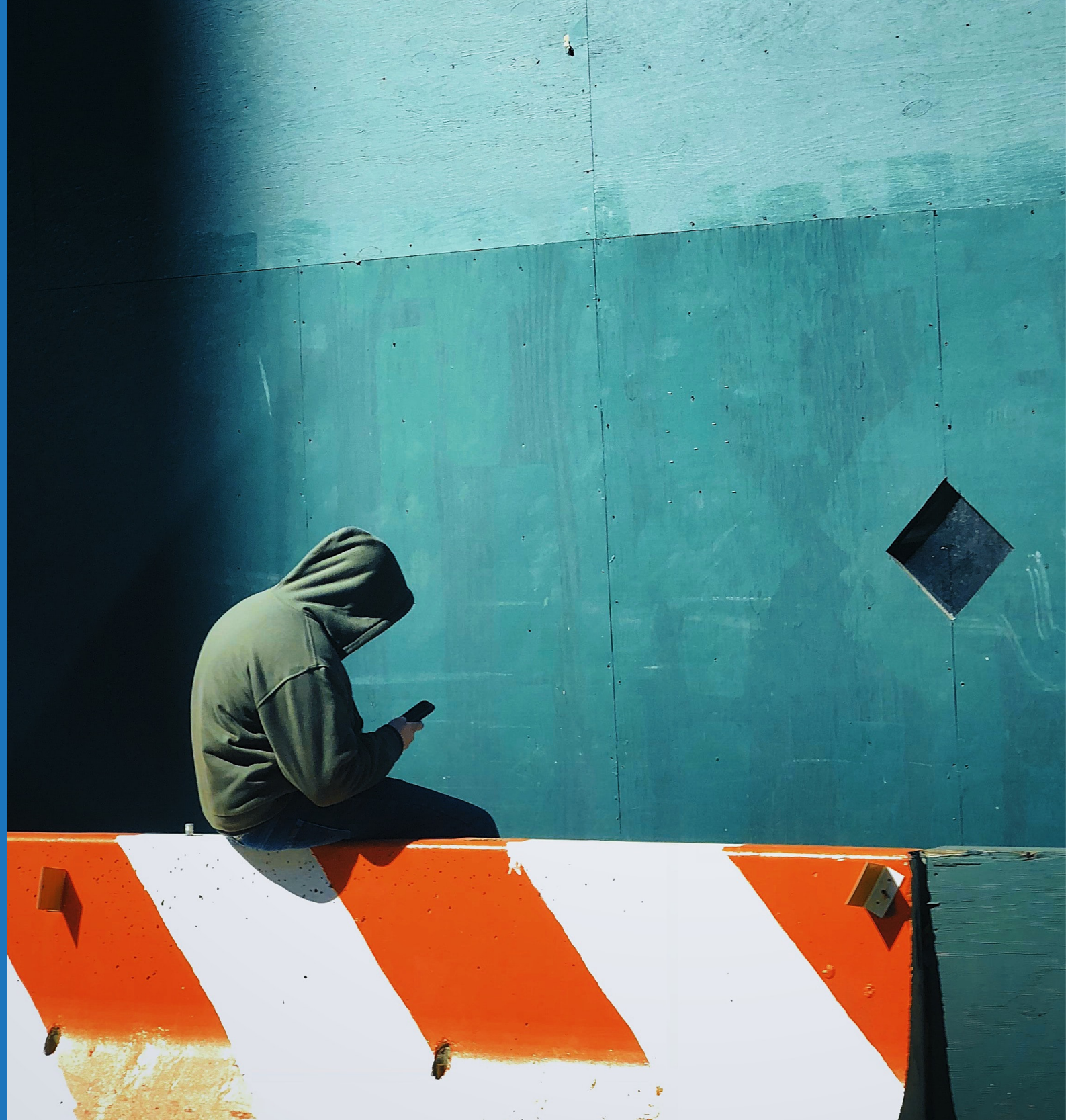
Lodrina Cherne

ASPEN TECH POLICY HUB

Technology Safety Initiative Operational Plan

Lodrina Cherne

Cover image by Robin Worral on Unsplash



Contents

Photo by Jon Tyson on Unsplash

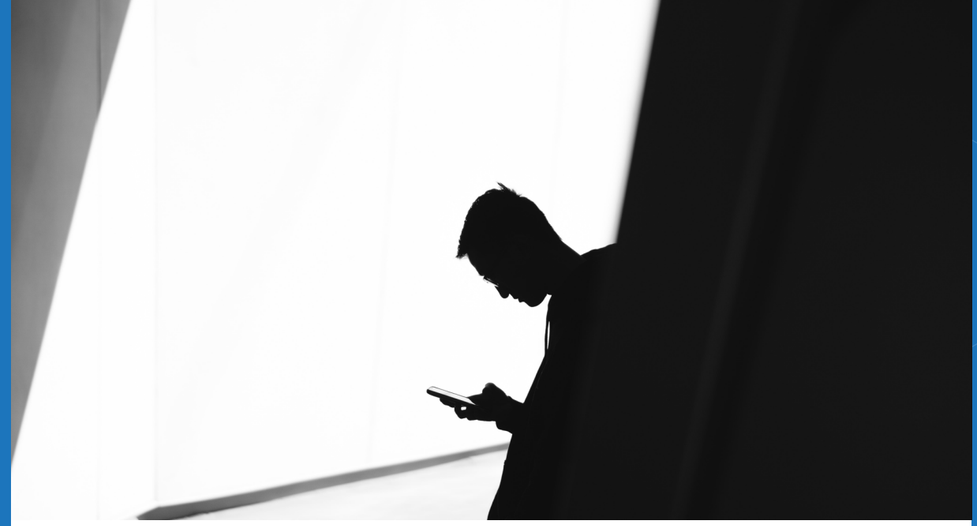


Image by Warren Wong on Unsplash

Executive Summary

What is the Technology Safety Initiative?

The Technology Safety Initiative is a proposal for the Department of Justice's Office on Violence Against Women to convene experts across the Federal Government and the private sector to address the harms of technology-enabled domestic violence and stalking. These experts in domestic violence, stalking, and technology would compile and consolidate resources for combating technology-facilitated abuse. The final output of the initiative would be a website for service providers and their clients that serves as a one-stop shop for those resources, including legal support and holistic approaches to safety planning. The initiative would ultimately provide a safe haven for people experiencing harassment and surveillance via technology.

How to Use This Operational Plan

The purpose of this document is to help the Office on Violence Against Women at the Department of Justice (DOJ) establish the Technology Safety Initiative and its associated website. Stakeholders can use this plan to understand the goals and components involved in the initiative. A project manager can use this guide to help establish the initiative.

Background: Technology Safety Initiative

Importance of the Technology Safety Initiative

The Technology Safety Initiative would address 2 major issues facing survivors of tech-facilitated abuse and their service providers:

- Survivors and their service providers do not have a clear place within the Federal Government to turn to for resources around technical safety and combating technology-facilitated abuse.
- Survivors can become overwhelmed by the technical aspects around finding safety.

- **Survivor** refers to someone who has experienced or is experiencing technology-facilitated abuse. The term "survivor" is used in this document instead of "victim" to highlight the ability of an individual to persevere through their abuse.
- **Service providers** refers to organizations working to support survivors. These are often civil society organizations, like domestic violence shelters, but they can range from nonprofits to law enforcement agencies.
- **Technology-facilitated abuse** is defined as "an abusive or harmful act or course of conduct facilitated through digital media"[1] which often combines the harms of domestic violence and stalking when performed through devices like cellphones and computers. Because of the overlap with domestic violence and intimate partner violence, this is a problem that disproportionately affects women and marginalized communities.[2]

Image by freestocks on Unsplash

Audience

The primary consumers of information at the Technology Safety Initiative website would be service providers looking for resources to help their clients who may be experiencing harms. These organizations would include:

- Domestic violence organizations
- Survivor service organizations
- Law enforcement agencies at the local, state, and federal levels

Resources on the website would include definitions of technology-facilitated abuse, safety planning information, advice about technology security, and information about applicable laws.

The secondary consumers of information from the website would be people seeking resources because they or someone they care about may be experiencing technology-facilitated abuse.

Convening Authority

The Technical Safety Initiative is a proposed project under the Justice Department within the Office on Violence Against Women (OVW). The director of OVW should appoint a dedicated project manager to lead the initiative and carry out the phases of this plan.

Image by Manny Becerra at Unsplash

The Justice Department houses numerous programs that tangentially focus on technology-facilitated abuse topics, including cyberstalking and stalkerware. These include the Federal Bureau of Investigation (FBI), National Criminal Justice Reference Service (NCJRS), National Institute of Justice (NIJ), Office for Victims of Crime (OVC), Office on Violence Against Women (OWV), U.S. Attorneys (USA), and the Bureau of Justice Statistics. Survivors and survivor-supporting organizations would benefit from many of these resources being consolidated under one initiative.

Budget

The DOJ Office on Violence Against Women can use FY2022 funding from the Emerging Issues in Violence Against Women program to establish the Technology Safety Initiative.[3]

Phases

Spearheading the Technology Safety Initiative and publishing the initial website would require the OVW to complete the following 4 phases:

- **Phase I: Establish Initiative**
- **Phase II: Secure Funding**
- **Phase III: Convene Experts**
- **Phase IV: Publish and Update Website**

Phases I and II can be performed in tandem and should take about 3 months. Phase III of convening experts should take about 5 months, and an initial version of the Technology Safety Initiative website would be published within one year of project start.

3 months	5 months	Remainder of year
Phase I: Establish Initiative	Phase III: Convene Experts	Phase IV: Publish Website
Phase II: Secure Funding		

After the initial website is published, OVW must promote the site, expand the site's reach and topics, and pursue permanency:

- **V: Promote Website**
- **VI: Improve and Expand the Technology Safety Initiative**
- **VII: Pursue Permanency**

Phases V through VII will be ongoing.

Phase I: Establish the Technology Safety Initiative

Formalize Mission

To create the Technology Safety Initiative, OVW will need to establish a mission statement. An example statement could be:

Focusing on the digital aspects of stalking and intimate partner violence by bringing experts together to help service providers and survivors combat technology-facilitated abuse.

The Technology Safety Initiative can be deemed successful if every conversation about safety and security for domestic violence survivors in the Federal Government includes a mention of digital stalking, harassment, and surveillance as well as ways to combat these harms.

Initial Topics: Technology-Facilitated Abuse

The Technology Safety Initiative should begin by addressing the most pressing issues at the intersection of technology, domestic violence, and stalking: cyberstalking, nonconsensual device monitoring, and stalkerware.

In Phase VI, additional topics are suggested for future phases. These topics might include harassment, nonconsensual pornography/nonconsensual image abuse, doxing, and swatting.

Image by Azat Satlykov on Unsplash

Phase II: Secure Funding

Securing Initial Funding

The DOJ's 2022 budget for OVW allocates $5 million for a new Emerging Issues in Violence Against Women program to "design and implement demonstration initiatives and other special projects that address emerging trends and unmet needs relating to gender-based violence."[4] At the time of budget allocation, there were "no current services" for this funding.

We recommend earmarking $750,000 of this Emerging Issues budget toward establishing and launching the first version of the Technology Safety Initiative and website.

This funding should go toward appointing a program staff member to be a point of contact for managing the initiative's budget, convening experts, and coordinating with a to-be-established web team to oversee Phases I–IV, and creating a framework for Phases V–VII.

Phase III: Convene Experts to Review Resources

Working Groups Assess Resources

Experts from the Department of Justice and social service organizations should come together in a series of working groups to assess how their resources complement one another and to identify resource gaps for combating tech-facilitated abuse.

These could include the organizations named in sections (b) "Department of Justice Tech Abuse Resources" and (c) "Civil Society Resources." It is particularly important to include representatives from DOJ including the FBI, NCJRS, NIJ, OVC, OWV, USA, and the Bureau of Justice Statistics. Civil society representatives should be invited from established programs including the National Network to End Domestic Violence Technology Safety project and the Clinic to End Tech Abuse.

Each organization should be represented by a primary representative and 1 or 2 deputies. The working group should be convened monthly, with committee work in additional meetings as needed to accomplish objectives.

To assess resources, the working group should:

- Identify relevant guides, research, reports, or other resources in their organizations related to tech-facilitated abuse;
- Assess how these resources complement the mission of the Technology Safety Initiative;
- Perform a gap analysis and identify missing resources for the website's users;
- Prioritize which gaps are the most important to address; and
- Work across organizations and create an initial plan to fill the gaps identified.

Department of Justice Tech Abuse Resources

Although OVW does not currently focus on technology-facilitated abuse or cyberstalking, information about these topics exists at many DOJ agencies. The Technology Safety Initiative can convene existing resources around technology and stalking from multiple agencies including the FBI and NIJ. Examples include:

Agency	Description
FBI	Cyberstalking case examples
NCJRS	Online harassment and cyberstalking report
NIJ	Needs assessment for technology-facilitated abuse
OVC	Stalking help brochure that includes technology-facilitated stalking
USA	United States Attorneys' Bulletin that includes information on cyberstalking and other cyber crimes
Bureau of Justice Statistics	Stalking statistics that include information on tech-facilitated stalking

Civil Society Resources

Expertise of OVW grantees should also be included as resources to review during the working groups. These include:

Organization	Description
National Center for Victims of Crime	A resource center that serves people harmed by crime
National Network to End Domestic Violence Technology Safety project	A network that provides technology safety planning and resources, including a survivor tool kit

Additional civil society organizations working in this space should be invited to contribute resources. Examples include:

Organization	Description
Clinic to End Tech Abuse	A New York-based program helping survivors in association with the New York City Mayor's Office to End Domestic and Gender-Based Violence
Coalition Against Stalkerware	A coalition of corporations, nonprofits, and research institutions to share information to stop and deter stalkerware
End Tech Abuse Across Generations	A California-based program that includes safety tool kit resources with a special focus on youth survivors
HackBlossom	Threat modeling and technical advice
Operation Safe Escape	A group of technical volunteers who assist individuals experiencing technology-facilitated abuse with technology-based advice
HeartMob by Hollaback!	Community-based online harassment support

A mockup flier that can be shared with civil society organizations to encourage them to share resources and participate in the working group can be found in the Appendix.

Phase IV: Publish a Technology Safety Initiative Website

Components and Content

Purpose

The purpose of the Technology Safety Initiative website would be to centralize resources around technology-facilitated abuse and share safety planning resources for service providers and survivors. This website would serve as a one-stop shop for resources to combat all types of tech-enabled abuse, including resources from OJP and other organizations across the federal and private sectors. The first version of the site should be a simple, easy-to-navigate place for service providers and survivors to find resources around guidance, statutes, and other material to facilitate safety planning.

Definition of Technology-Facilitated Abuse

The Technology Safety Initiative website should include a definition of tech-facilitated abuse to better inform users of what this abuse looks like. The site should use the definition from a 2020 NIJ-sponsored report on technology-facilitated abuse, which we use in this report and which defines technology-facilitated abuse as an "abusive or harmful act or course of conduct facilitated through digital media (e.g., websites, social networking platforms, dating sites, apps, blogs, online games, instant messages, email) and targeted either directly or indirectly at a particular person or group of persons, often (but not always) with the intent to cause emotional distress, reputational damage, and/or fear for personal safety."[5]

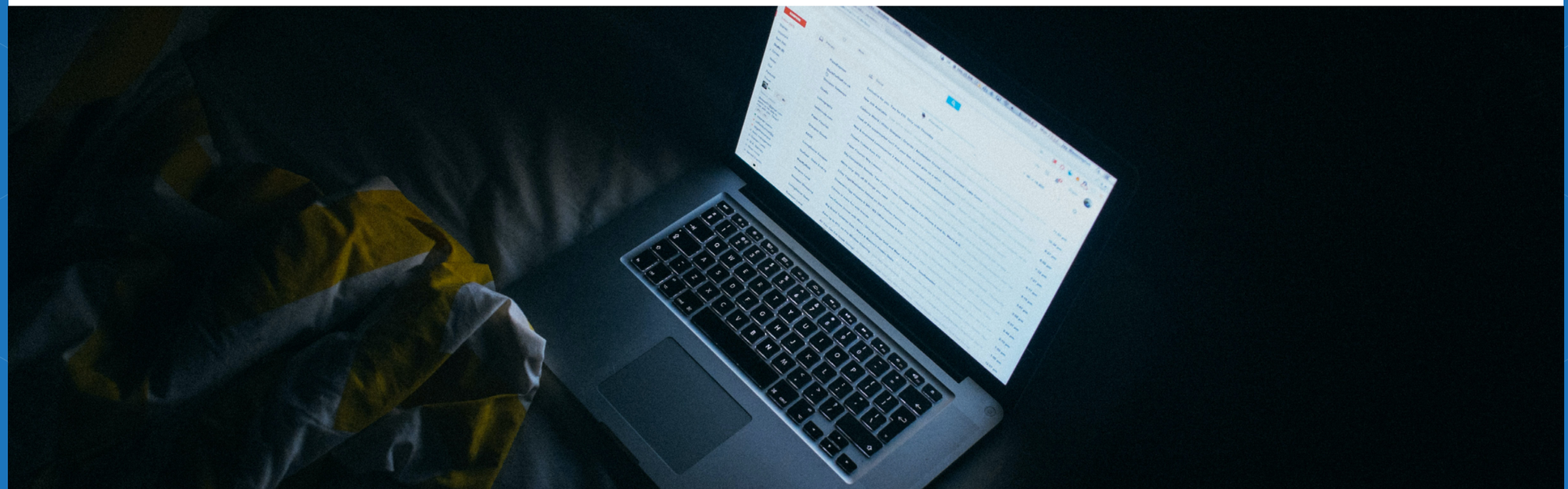
Example Concerns Related to Technology-Facilitated Abuse

The website should also include example concerns of people being monitored without their consent. These examples might include: suspicions that their partner is nonconsensually monitoring their location; indications that personal email or messages are being read without consent; or suspicions that private conversations are being eavesdropped on. These concerns might overlap with technical issues like a phone battery dying quickly, suspicious apps appearing on devices, or a review of online accounts that shows unauthorized activity.

Safety Planning

The Technology Safety Initiative website should include advice, based on information from experts convened, about what service providers and survivors can do when experiencing tech abuse. Because each individual situation is unique and there is no one right course of action, such advice should take into account *threat modeling*, defined more in subsequent sections.

Image by Jay Wennington on Unsplash



DIGITAL SECURITY ADVICE FOR SURVIVORS AND THOSE SUPPORTING THEM

Digital security should be considered at every step of the process around survivor safety. Just like other domains such as physical security, promoting digital security concepts is key to empowering people experiencing technology-facilitated abuse. The Technology Safety Initiative website should be sure to spell out specific security recommendations for survivors and their supporters. Here are some of these recommendations.

FOR SURVIVORS

Security advice from the cybersecurity world can be used to help survivors plan their digital approach to safety.

Threat Modeling

- *Threat modeling* is prioritizing recommendations based on the greatest harms and needs identified for a particular situation.[6] Rather than worrying about all the "what ifs" of safety, focus on the biggest threats and create a plan to address them.
- Survivors should be sure to create their own threat models. If your biggest concern is keeping your phone calls private, for example, you might consider putting a secure passcode on your phone, using a different phone altogether, or setting up a software-based virtual phone number like Google Voice.

Intrusion Analysis Modeling

- *Intrusion analysis modeling* is modeling the path of a criminal hacker during a computer break-in. Examples include the Cyber Kill Chain or MITRE ATT&CK.[7,8] These models show how the longer an attacker spends in a computer system, the more damage they do. Cybersecurity practices focus on stopping an attacker early in their hack. This concept can be applied to personal safety.
- Take an example of a survivor worried that a partner may place stalkerware on their phone. Intrusion analysis would advise this individual not to allow their partner physical access to their unlocked phone, as this would prevent the installation of stalkerware.

Digital Hygiene: MFA, Reviewing Settings and Logins, Installing Updates, Limiting Information Online

Planning for digital safety and practicing good digital hygiene help keep your online accounts and devices secure. See below for some digital hygiene strategies for survivors. Just like personal health and hygiene, these strategies are basic concepts that survivors would be advised to revisit regularly.

- **Install Multifactor Authentication** Multifactor authentication (MFA) or 2-factor authentication (2FA) involves logging into accounts with multiple credentials, usually a password and something like a code texted to your phone. MFA and 2FA can help keep your accounts secure because even if someone knows your password, they don't have the second login code.
- **Review Account and Application Settings** Regularly review settings for online accounts as well as phone and tablet apps for privacy and sharing options. You should specifically ensure that your email addresses do not have permission to access your data and that applications are not sharing microphone and camera settings.
- **Review Account Logins** Many email services will allow you to see what devices are logged into your account. This allows you to easily tell if someone else is looking at your personal information. For example, if you use only Apple devices but see your account is signed in on a device that uses Windows, you may realize someone else is looking at your information and you may choose to strengthen your security using other digital hygiene concepts.
- **Install Software Updates** Installing updates is a good way to keep phones, tablets, and computers secure. On iOS and Android devices, or Mac and Windows computers, security updates are typically done along with usability and feature updates.
- **Limit Information Shared Online** Limiting personal information shared online may help protect your online accounts. While there is no definitive guidance on what to share on social media, good cyber hygiene limits personal information sharing, which prevents someone with malicious intent getting information to reset your passwords or learning about your routines.

Note: These recommendations are context-dependent. For example, some survivors may not choose to have a unique password or turn on MFA if they are worried it might raise an abuser's suspicions.

FOR THOSE SUPPORTING SURVIVORS

Security approaches like threat modeling, intrusion analysis modeling, and digital hygiene techniques may also be new for service providers, legal aid, law enforcement, or others helping survivors. Some security concepts for supporters to consider are:

Understanding Needs

Every survivor will have different concerns for digital safety, so be sure to tailor your approach to each survivor. Some common requests that survivors may make to support organizations include:

- **Preserving Data for Court** If a survivor asks you to preserve data for a court case, one option is to seek out a specialist in digital forensics. Digital forensics experts can help you preserve data so digital messages, apps, and devices can be captured for future legal action.
- **Securing Devices** If a survivor asks you to help them secure devices, look at the tips in the "For Survivors" section above. Those with cybersecurity skills who are unfamiliar with digital security for personal safety may also wish to follow guides for securing Android phones such as the Clinic to End Tech Abuse's "Android phones" resource guide or Apple's "Device and Data Access when Personal Safety Is at Risk" documentation.
- **Nondigital Safety** If a survivor has a concern about digital monitoring, they may also have other more pressing safety concerns. Seek to refer survivors to traditional domestic violence support organizations as needed.

Seeking Security Training

Different professional organizations and communities have different opportunities and needs to seek digital security training. Search out cybersecurity training opportunities specific to your specialty.

Note: Even if supporter-survivor networks are not familiar with cybersecurity concepts, supporters can create referral networks with local technology experts to aid them in providing digital assistance.

Image by Philipp Katzenberger on Unsplash

Guides and Resources

The Technology Safety Initiative website should include guides for safety planning, technical advice, and contact information for support hotlines, advocacy groups, or law enforcement agencies. Ideally, the site would have a system that specifies the type of resource or referral needed based on a user's specific situation (whether they are a service provider or survivor). See Figure 1 as an example.

The website should feature a search function that pulls up law enforcement and social service contact information based on a survivor's address. It should also include state-specific resources, such as relevant agencies by state that receive OVW funding. OVW already stores much of this information on its website.

Applicability of Criminal Laws

The Technology Safety Initiative website should include information about laws and statutes that may be relevant for survivors. Any information regarding laws should take into account safety planning and threat modeling, and should make clear that legal recourse may not always be appropriate for an individual.

While technology-facilitated abuse is not specifically seen as a federal crime, multiple laws may apply to survivors experiencing nonconsensual device monitoring and cyberstalking, which are federal crimes. Additional criminal laws that may apply include:

- 18 U.S.C. § 2261A: Cyberstalking
- 18 U.S.C. § 875: Threats and extortion
- 47 U.S.C. § 223: Obscene or harassing telephone calls
- 18 U.S.C. § 1030: Computer hacking

A review of state laws and statutes should be included as well.

User Journey

Recommended User Interface

The user journey of the website should be developed based on the results of the expert convening that occurs during Phase III. Nevertheless, there are some guiding principles that should inform the user journey. The User Interface (UI) should:

- Give actionable next steps for safety planning with minimal instruction on how to navigate the website; and
- Minimize harm by adding UI features that allow a survivor to find help quickly or to swiftly exit the website.

One way the website might connect the right user to the right recommended resources is through question prompts. Users can be prompted through a series of questions asking them to select from pre-populated answers:

- Who are they? *Options include service provider or individual.*
- What are they looking to do? *Options include finding help or learning about resources.*
- What additional concerns do they have? *Options include finding someone to talk to, securing devices, documenting experiences, or getting in touch with law enforcement.*

After options are selected, the website can dynamically load relevant content below the selections on the same page, or direct the user to a new webpage with relevant content displayed.

Because safety planning will differ based on who the user is or what their threat model is, different content can be displayed for different users.

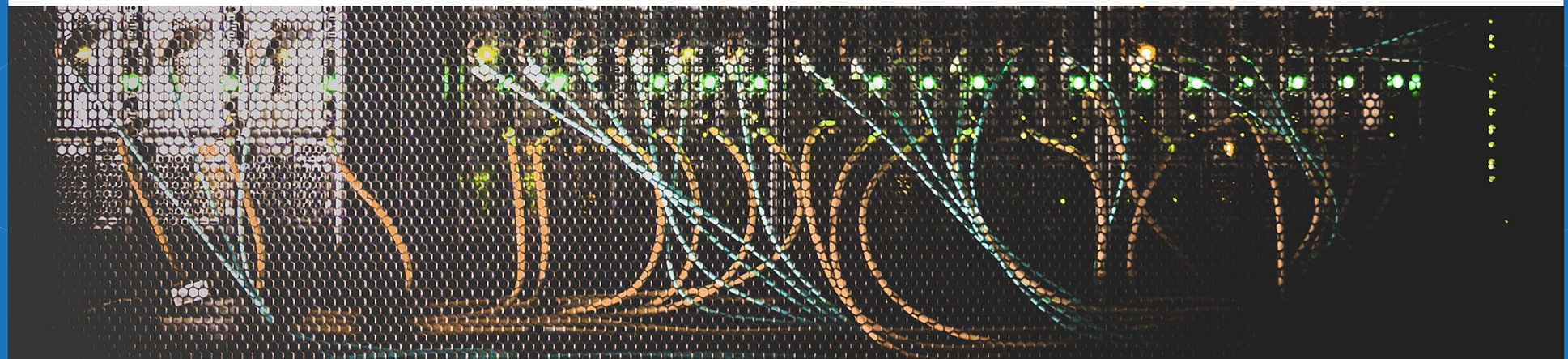
Figure 1: Website Example Options

Technical Requirements

Building and Updating the Website

Options for creation of the website include using the existing web team for DOJ OVW or partnering with tech-focused agencies like the US Digital Service (USDS) and the General Services Administration's 18F.

Image by Taylor Vick on Unsplash



The website content should be regularly reviewed and updated at least quarterly as noted in "Phase VI: Expansion of Technology Safety Initiative." Updates should ensure that the most up-to-date version of hosted resources are available and that any links to third-party websites (non-Justice.gov sites) are still relevant.

Website Design Principles

Accessibility and usability should be considered in any website updates, consistent with the US Web Design System's modernized website requirements.[9]

User-centered design principles should be followed when designing the website. For example, designers should test the site on different types of audiences to see if they can access and understand relevant information.

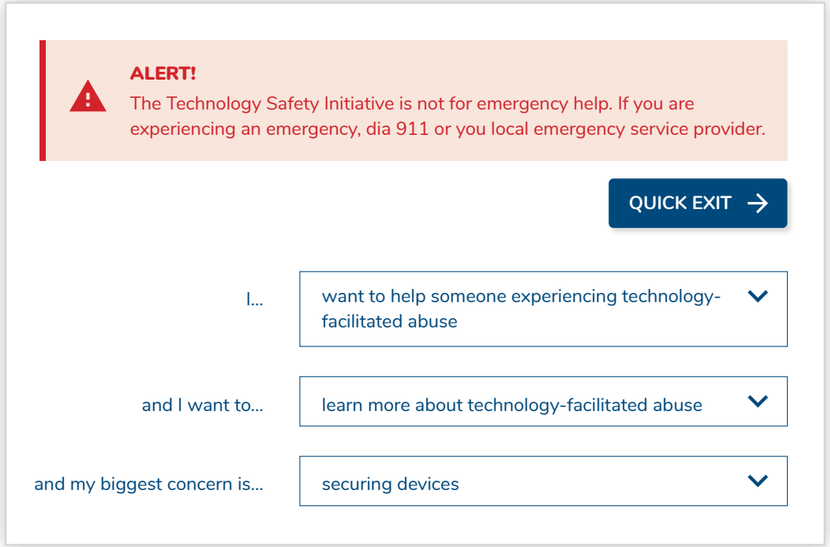


Figure 2: Banner and Quick Exit Example

Hosting Location

The initial Technology Safety Initiative website can be hosted as a subpage of the OVW website. An example URL could be: *justice.gov/ovw/tech-safety*.

Quick Exit

All pages on the website should have a "Quick Exit" function that immediately leaves the site by redirecting to an innocuous third-party site such as weather.gov (see Figure 2). This functionality can be seen on OVW's Domestic Violence page. The purpose of the "Quick Exit" function is to allow survivors to quickly exit if seeking help might be dangerous for them. While no foolproof solutions exist to address browser history monitoring, this is an easy way to increase safety.

Banner with Emergency Hotline

The Technology Safety site should have a banner displaying emergency help numbers (for example, 911) at the top of each page. Crisis services should be listed at the top of every page for those seeking emergency help. Even though the site should not be a substitute for emergency or crisis services, adding contact information for these is critical for providing resources.

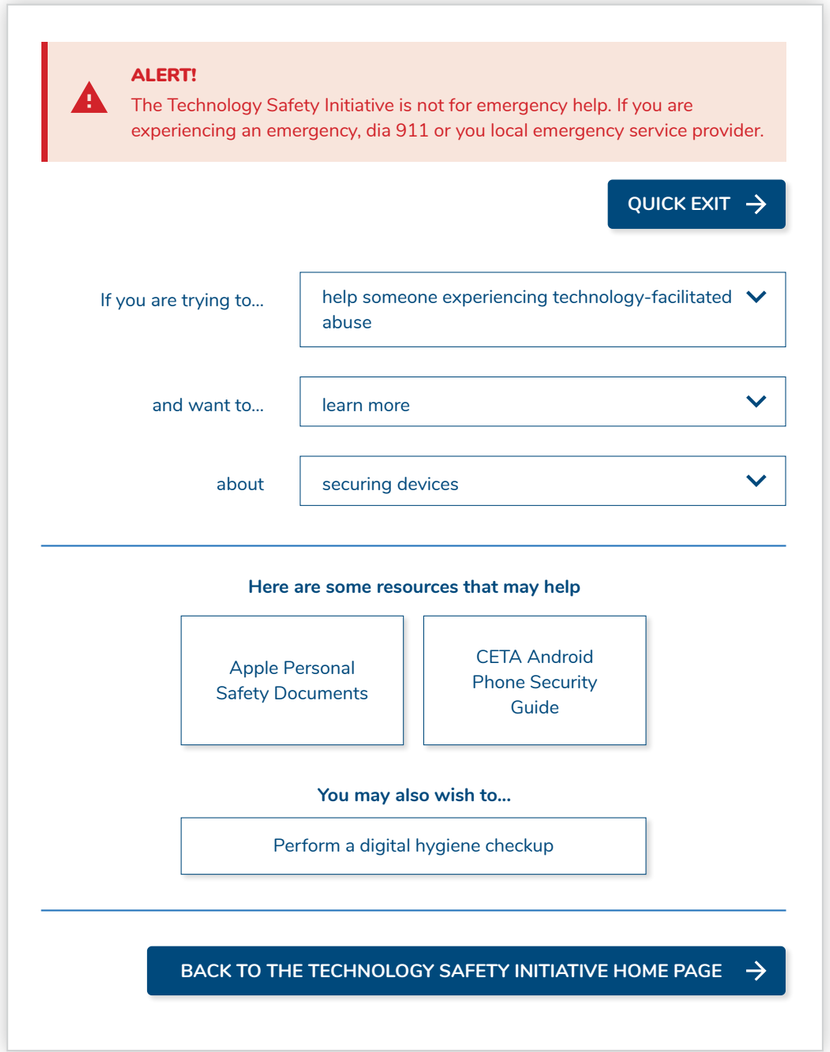


Figure 3: Example of Tailored Results

Phase V: Promote Website

Once the Technology Safety Initiative website has been created, OVW will need to promote it to survivors and service providers. This can be done via a multipronged approach:

Launch Campaign

The launch campaign can include a press release, social media campaign, and service provider amplification. The launch should be announced via press release, which can be hosted on the OVW Press Room page. Social media announcements should be made on multiple platforms (such as Instagram, Facebook, and Twitter).

Private sector organizations contributing resources to the website can help publicize the launch by amplifying press releases and social media announcements, as well as adding links to the Technology Safety Initiative site on their own websites.

Promote in OVW TTAC Training

OVW Training and Technical Assistance Center (TTAC) trainings for grantees should include and/or reference the Technology Safety Initiative website, sharing it as a resource with service providers when they request training. This would capitalize on the technical expertise that TTAC already offers grantees who are looking for technical assistance with their programs. TTAC can also host webinars for grantees to describe who can benefit from the resources available at the website.

Tie to Existing Gender-Based Violence Initiatives

Service providers can promote the Technology Safety Initiative website in yearly campaigns around gender-based violence, such as during Domestic Violence Awareness Month (October), International Day for the Elimination of Violence against Women (November), and Stalking Awareness Month (January).

Success Metrics

OVW should measure how successful this new consolidated website approach is. Performance indicators can be measured through website traffic (a passive measure) and through surveying service providers on the site's usefulness (an active measure).

Webpage traffic to the Technology Safety Initiative homepage can be measured for total traffic volume and referrals from internal (.gov) and external (all other nongovernment) web pages. A website administrator can pull monthly traffic statistics to understand whether traffic is increasing and the site is being used.

Phase VI: Improve and Expand the Technology Safety Initiative

Content on the Technology Safety Initiative website should be iterated upon. In addition, the working group and web developers should ensure that the website is updated quarterly on the latest issues being raised in the domestic violence prevention, stalking prevention, and technology communities. These teams should also repeat phases III (convening experts) and IV (publishing and updating the website) annually. As the program matures, additional stakeholders from the public and private sectors should be convened monthly, topics related to tech-facilitated abuse should be expanded, and the website should be matured to reach more people.

Expansion of Topics

As the program matures, additional technology-facilitated abuse harms such as sextortion, nonconsensual image abuse, doxing, and other topics including those addressed in the 2020 NIJ-sponsored report on technology-facilitated abuse should be included. Definitions for these terms can be found below.[10]

- *Harassment* can refer to physical threats, sexual harassment, stalking, and sustained harassment, as defined by the NIJ.
- *Nonconsensual Pornography/Nonconsensual Image Abuse* refers to the nonconsensual release of explicit photos of an individual online.
- *Doxing* refers to the nonconsensual release of personal information like name and address online.
- *Swatting* refers to faking the report of a crisis in order to falsely deploy emergency services to a specific location.

Expansion of Working Group Participants

After the initial website is published, an additional call for federal stakeholders should be performed to add working group stakeholders outside of DOJ whose work is relevant to the Technology Safety Initiative.

Agencies that have worked in this space include the Federal Trade Commission (FTC) and Government Accountability Office (GAO), which have written reports on the use of tracking apps and mobile software.[11]

An additional call for social service organizations to contribute resources should be circulated as well; see the sample flier in the Appendix.

Expansion of Audience

The audience of the Technology Safety Initiative website can be expanded in subsequent iterations. This includes creating resources for allies (friends and family who may be helping someone experiencing tech-facilitated abuse) and expanding the reach of existing resources by providing materials in multiple languages. Support for additional languages should be consistent with guidelines in the Language Access Plan for the Office on Violence Against Women.[12]

Phase VII: Pursue Permanency

During the first year of the Technology Safety Initiative, OVW should consider how to continue to fund the program in future years. The OVW team should estimate how much it will need to sustain the initiative, examine if additional Emerging Issues in Violence Against Women funding will continue to be available, and determine whether funding for the program will need to come from outside OVW.

OVW can look to more established programs where the Justice Department has participated in cross-department coordination for examples of how to mature, fund, and staff the Technology Safety Initiative. These include:

- The Elder Justice Initiative, which coordinates the Department of Justice's efforts to protect older adults.
- StopBullying.gov, an anti-bullying resource site that is a joint effort of the departments of Justice, Education, and Health and Human Services.

Appendix: Service Provider Mockup

Endnotes

1 Amanda R. Witwer et al., "Countering Technology-Facilitated Abuse: Criminal Justice Strategies for Combating Nonconsensual Pornography, Sextortion, Doxing, and Swatting," National Institute of Justice, January 2020, https://nij.ojp.gov/library/publications/countering-technology-facilitated-abuse-criminal-justice-strategies-combating.

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

3 "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.

4 *Id.*

5 "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 Victoria Drake, "Threat Modeling," The OWASP Foundation, accessed February 1, 2022, https://owasp.org/www-community/Threat_Modeling.

7 "The Cyber Kill Chain," Lockheed Martin, accessed February 1, 2022, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

8 "Enterprise Matrix," MITRE ATT&CK, accessed February 1, 2022, https://attack.mitre.org/matrices/enterprise/.

9 "21st Century Integrated Digital Experience Act: What Does It Mean to Modernize Websites?," Digital.gov, last modified August 31, 2020, https://digital.gov/resources/21st-century-integrated-digital-experience-act/#what-does-it-mean-to-modernize-websites.

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

11 "Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking," US Government Accountability Office, last updated May 9, 2016, https://www.gao.gov/products/gao-16-317; and "Who's Stalking: What to Know About Mobile Spyware," *Consumer Information Blog*, US Federal Trade Commission, September 26, 2016, https://www.consumer.ftc.gov/blog/2016/09/whos-stalking-what-know-about-mobile-spyware.

12 "Language Access Policy and Plan," Office on Violence Against Women, last updated January 18, 2017, https://www.justice.gov/ovw/page/file/930326/download.

ASPEN TECH
POLICY HUB

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