Chapter 38

As Technology Evolves, so Does Domestic Violence: Modern-Day Tech Abuse and Possible Solutions

Eva PenzeyMoog and Danielle C. Slakoff

Abstract

The reality of domestic violence does not disappear when people enter the digital world, as abusers may use technology to stalk, exploit, and control their victims. In this chapter, we discuss three unique types of technological abuse: (1) financial abuse via banking websites and apps; (2) abuse via smart home devices (i.e., "Internet of Things" abuse); and (3) stalking via geolocation or GPS. We also argue pregnancy and wellness apps provide an opportunity for meaningful intervention for pregnant victims of domestic violence.

While there is no way to ensure users' safety in all situations, we argue thoughtful considerations while designing and building digital products can result in meaningful contributions to victims' safety. This chapter concludes with PenzeyMoog's (2020) "Framework for Inclusive Safety," which is a roadmap for building technology that increases the safety of domestic violence survivors. This framework includes three key points: (1) the importance of educating technologists about domestic violence; (2) the importance of identifying possible abuse situations and designing against them; and (3) identifying user interactions that might signal abuse and offering safe interventions.

Keywords: Financial abuse; stalking; coercive control; smart home device abuse; pregnancy apps; inclusive safety

The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 643–662

doi:10.1108/978-1-83982-848-520211047

Introduction

People who work in tech define rare instances of user harm as "edge cases." In tech, defining an issue as an "edge case" can be used as an excuse to ignore the issue; it is not worth fixing because only a small number of people will be impacted (Meyer, 2020). Domestic violence is not an "edge case." Globally, 137 women are killed by a member of their household each day (United Nations Office on Drugs and Crime, 2018). In reality, domestic violence is common, and technologists (designers, programmers, project managers, and others who influence the creation of digital products) must acknowledge its reality and plan for it within products.

Domestic violence refers to violence at the hands of a family member, roommate, intimate partner, or someone else in one's domestic setting (United States Department of Justice, n.d.a). Intimate partner violence (IPV) refers to violence at the hands of a current or former intimate partner (World Health Organization, 2017). The World Health Organization (2017) found one-third of women will experience intimate partner violence worldwide, and 90 to 95 percent of IPV involves a male perpetrator and female victim (Belknap & Melton, 2005). Intimate partner violence in the United States (US) cuts across all genders, races, and social classes (Petrosky, Blair, BetzFowler, Jack, & Lyons, 2017) and includes physical, financial, emotional, sexual, and psychological abuse.

The reality of domestic violence does not disappear when people enter the digital world, as abusers may use technology to stalk, exploit, and control their victims. In this chapter, we use vignettes to discuss three types of technological abuse: (1) financial abuse; (2) abuse via smart home devices; and (3) stalking via geo-location or GPS. We also argue pregnancy and wellness apps provide an opportunity for meaningful intervention for pregnant victims of domestic violence.

While there is no way to ensure users' safety in all situations, we argue thoughtful considerations while designing and building digital products can result in meaningful contributions to victims' safety. We also argue that PenzeyMoog's (2020) "Framework for Inclusive Safety," included in this chapter, provides a roadmap for building technology that increases the safety of domestic violence survivors.

As a technologist who speaks at public events, PenzeyMoog is sometimes approached by survivors of technology-related abuse. The scenarios and vignettes in this chapter draw upon the victims' experiences as described in these casual conversations. The vignettes (and all dialog) are *not* word-for-word descriptions of events, but instead serve to illustrate key concepts in the chapter. All conversations occurred between 2017 and 2019, and all identifying information has been removed.

Coercive Control and Technology-Facilitated Intimate Partner Violence: A Brief Summary

"Coercive control" is an aspect of intimate partner violence that includes emotional terrorism and the continued dominance of one person over another person (Stark, 2006, 2007). Coercive control features both implicit and explicit intimidation and threatening behaviors by the perpetrator (Stark, 2006, 2007) and an emphasis on limiting the victim/survivor's independence (Robertson & Murachver, 2011). In the wrong hands, technology can be used to increase a perpetrator's control over a victim/survivor's life by limiting her independence and instilling fear (Douglas, Harris, & Dragiewicz, 2019). Importantly, technology-based domestic abuse is very likely an additional form of abuse perpetrated in the relationship (Harris, 2018; Lyndon, Bonds-Raacke, & Cratty, 2011).

In her seminal study of domestic violence support practitioners in Australia, Woodlock (2013) found almost all (98%) had assisted a survivor of intimate partner violence with technology-based abuse. Moreover, during in-depth interviews with 30 female victims/survivors, George and Harris (2014) discovered each one had experienced some sort of abuse or surveillance through technology. Importantly, instances of technology-related stalking – often featuring unwanted phone calls and surveillance – are a risk factor for domestic homicide (McFarlane, Campbell, & Watson, 2002). Along the same vein, the Queensland Domestic and Family Violence Death Review and Advisory Board (2017) acknowledged that technology-facilitated abuse was "an emerging trend" across cases of domestic homicide (p. 2). Simply stated, technology-facilitated abuse must be taken seriously as a form of oppression and control.

Financial Abuse

Financial abuse is among the most powerful methods abusers have to keep a survivor in a relationship and to diminish their ability to safely leave (National Network to End Domestic Violence, 2014). According to a study of survivors enrolled in a financial literacy program in the United States (Postmus, Plummer, McMahon, Murshid, & Kim, 2012), 94% had experienced some element of financial abuse while in their abusive relationship (see also National Network to End Domestic Violence, 2014). When someone is on an allowance, or when an abuser knows about all the purchases their partner makes, leaving the relationship can seem impossible. Simply put, many survivors do not know how they are going to survive financially if they leave (Hunter, 2006).

Shared or joint bank accounts are normally accounts meant for one person, but two people are given access. Often, a joint account has one login and password both parties use, one email address that receives updates, and one person whose identity gets verified whenever the system detects suspicious activity.

> Helen and Isaac opened a joint bank account. Isaac quickly took control of the pair's money. Each month, he created a budget, paid the bills, and moved their income into various savings accounts.
>
> When Helen logged into the joint account from a new computer or from a new Wifi network, she was faced with identity questions about Isaac, despite having the password. These questions asked about old addresses and house numbers. In order to access the account, she needed to ask Isaac for the answers. One day, he refused to give her the answers, saying he had their finances under control. She tried logging into the banking app on her phone, only to see that the password was changed. She could no longer access her money. (Case study 1)

Helen's experience is common. Often, survivors are not provided or allowed access to their own money (National Network to End Domestic Violence, 2014), and this compounds the survivor's reliance on the abuser. In this way, the survivor's lack of financial independence is yet another means of coercive control.

Importantly, there are some key ways technology design could work to reduce this type of financial abuse. Joint accounts should be accessible by both parties, and each joint account should have two separate logins as well as identity verification questions tied to each individual. Moreover, banks, credit card companies, and other groups who work within the personal finance space, should flag suspicious account activity that could point to financial abuse, such as constantly changing passwords in joint accounts.

When it comes to detecting financial abuse, much can be learned from the existing laws and practices around identifying and supporting victims of elder abuse (Allen, 2000; Chesterman, 2015). According to a memo sent from the Financial Crime Enforcement Network (2011) to members of the United States (US) Treasury, the following are some indicators of elder abuse:

- Changes in typical banking patterns.
- Erratic or unusual banking transactions.
- Frequent large withdrawals.
- Daily maximum currency withdrawals from an ATM.
- Sudden non-sufficient fund activity.
- Uncharacteristic nonpayment for bank or financial services.
- Uncharacteristic attempts to wire large sums of money.
- Closing certificate of deposit or bank accounts without regard to penalties.

These indicators of elder abuse are signs of financial abuse more generally. All customers who display these warning signs warrant some form of outreach. Customers could receive a call from a banker trained in financial abuse detection to discuss the troubling behavior. This communication could assist victims of financial abuse as they may not yet have recognized the abuse, or they may be unsure if the behavior is abnormal and abusive.

Credit card companies could do similar outreach. A common tactic of abusers is ruining the credit of their partner by opening credit cards and/or taking out loans in the name of their partner, which gives the abuser access to funds without the risk of ruining their own credit (Becky's Fund, n.d.). Customers who have been reliable credit card holders but suddenly open multiple accounts or have a lot of unusual account activity could receive a "check-in" call to ensure nothing is amiss. Of course, people in these industries should not make assumptions about whether abuse is occurring. Moreover, a survivor may not be safe enough to discuss it, or they may already be taking steps to safely leave the relationship. These phone calls, however, could be a starting point.

While the ideas above offer a proactive approach, reactive approaches are also important. Two major banks in Australia have created hotlines staffed with trained employees to assist customers experiencing domestic abuse (Commonwealth Bank of Australia, 2020; National Australia Bank Limited, 2020). Although these banks are taking a reactive approach to assisting financial abuse survivors (waiting for the customer to reach out for help), it is an important step other banks should model.

> Vivian, a customer at Australia's Commonwealth Bank reported that, when she told a customer support representative she was disentangling her finances from her soon-to-be ex-husband, the representative, without asking about intimate partner violence directly, asked her questions designed to keep a survivor safe, such as: "Is it safe to receive mail about the changes in banking at home?" and "Do you need assistance finding a new branch?". (Case Study 2)

In all US states except New York, workers at banks and other financial institutions are required to report suspected elder financial abuse to appropriate law enforcement, Elder Care Service providers, and/or human resource workers for the county (Stetson Law, n.d; US Department of Justice, n.d.b); these workers are empowered through training to recognize and support possible victims. This same protocol could be implemented for victims of IPV generally. Most states in the US have laws that define financial abuse of the elderly as a crime (Morton, 2018). However, there is no similar law defining financial abuse of an intimate partner as a crime. In other countries, such as Australia, financial abuse – in the context of family violence – is criminalized federally, as well as in the individual state and territory jurisdictions (see Australia's Family Law Act 1975 [Cth]).

US Senator Patty Murray introduced a bill in 2007 to the 110th Congress that would have strengthened financial protections for survivors of domestic violence, stalking, and sexual assault (GovTrack, 2007). The bill did not make it to a vote before the end of the 110th Congress, which meant that it was cleared from the books (GovTrack, 2007). Murray proposed a similar law in early 2019, and at the time of writing, there still has not been a formal vote on it (S.627 - SAFE Act of 2019). A law focused on the financial abuse of an intimate partner is an essential step toward helping people regain financial control during – or after – an abusive relationship. As it stands, lack of financial security is one of the primary reasons survivors do not leave or quickly return to an abuser (Sharp-Jeffs, 2015). Technologists in the financial sector have a significant opportunity to prevent abuse as well as recognize when it is happening and offer support.

Internet of Things/Smart Home Device Abuse

> Lisa and Ben use an Amazon Echo to connect to their Nest thermostat, Ring doorbell, and touchpad smart lock. Ben installed all of these devices. Lisa is home alone while Ben is traveling when the lights suddenly go out. She uses a phone app to turn them back on – and they go out again. Feeling scared, Lisa leaves the house, hoping that the issue with the lights will be over once she returns.

> When she returns home and enters the code into the touchpad on the front door's smart lock, the buttons flash red and the door remains locked. She tries again and, still, it is locked. She calls Ben. "Are you sure you're doing the right code? 1564?" Ben asks.
>
> "The code is 1546," says Lisa. "1564. Write it down. That's always been the code. You know I won't always be available when you forget things," said Ben, exasperated. Lisa is sure she knew the code, but drops it.
>
> Later, while making lunch, Lisa starts sweating. She looks at the Nest thermostat: it is set to 90°F. Suddenly, the phone rings. "Why do you have the temperature set to 90 degrees on the Nest? What the hell are you doing?" "I haven't touched it!" says Lisa. "I'm turning it down," says Ben. "Why can't you figure out these things? It's not that hard." He hangs up.
>
> Lisa is upset about the home device issues and how Ben is treating her. She calls her sister to talk through what's going on, and explains that Ben must be behind some of the issues. The chat is interrupted; Ben is calling again. She answers. Ben asks her how night is going and asks if she'd "talked to her sister lately?". Shocked, Lisa asks, "How did you know?"
>
> "It's just a question. Why are you so paranoid?". (Case Study 3)

Of course, Ben did know Lisa was talking to her sister. He knew because of an Amazon Echo feature that lets him use it as a listening device (Graham, 2019). The "drop in call" feature is useful in some situations. For example, if someone is at home and their phone is dead or in another room, their partner can call them through the drop-in feature. If prior "permission" has been granted, the Amazon Echo simply gives an alert of an incoming call, and the call starts. With the use of an Echo Show (Amazon's tablet), an abuser can create a makeshift home security system that lets you "drop in" on various tablets around the house. This is how Ben monitors Lisa's activity.

Ben was "gaslighting" Lisa by controlling all the smart home devices from apps on his phone. He made Lisa think she was losing touch with reality – she couldn't trust her own experience (Stark, 2019). Gaslighting is a form of psychological abuse where an abuser causes harm and then denies the harm, causing confusion for the victim/survivor (Stark, 2019; Sweet, 2019). Gaslighting is a common form of psychological abuse used against domestic violence victims and reaffirms one person's power over another by causing the victim to feel like they are "going crazy" (Sweet, 2019). Smart home devices gave Ben new opportunities to gaslight Lisa.

According to the research firm Statista (2020), over half of all US households will have at least one smart home device by 2024. As such, abuse through smart home devices is becoming, and will continue to become, increasingly common

(Bowles, 2018). Domestic violence helpline workers polled in 2018 reported an increase in calls focused on smart home devices since 2017, and lawyers are currently working on how to include smart home devices in restraining orders (Bowles, 2018).

Eva Galperin, the Electronic Frontier Foundation's Director of Cybersecurity, explains that abusers often restrict access to necessary apps and choose not to educate their victims about how the product works (Bowles, 2018). She explains: "They're not sure how their abuser is getting in and they're not necessarily able to figure it out because they don't know how the systems work" (as cited in Bowles, 2018, para 24). Sometimes abusers will not set up the necessary app on their victim's phone, or they will withhold passwords in order to ensure control over the product. Victims with knowledge of – and access to – the product are in a better position to stop and recognize the abuse.

Attorney Alexis Moore, a cyberstalking expert, described working with a client whose abuser "would remotely turn on the heat in the survivor's house" during the hottest days of the year, "just to unnerve her and remind her he was in control" (as cited in Kippert, 2019, para 4). Moore described another abuser who would remotely unlock a survivor's home and car doors and then would describe her as an unfit parent for not being able to maintain security (Kippert, 2019). Moore further described abusers listening to their victims through Amazon Alexas and Echos, smart TVs, and home security cameras (Kippert, 2019).

One way to prevent gaslighting and abuse via smart home devices is to include an "activity log" within the user interface. At the time of writing, Nests do not show the user this information. An activity log – which would include what time a user changed the temperature – would provide a timeline of activity to the victim. Moreover, an activity log could help victims explain and prove technological abuse to law enforcement.

Importantly, technologists must explore the potential for abuse in the "activity log" fix. Potentially, abusers could use these logs to keep tabs on victims (e.g., determine their victim's comings-and-goings via the thermostat). While a valid concern, we believe giving the victim the power to fight gaslighting and have "proof" of abuse for police or legal proceedings is an important step. Until all smart home devices show history logs, survivors should make efforts to record smart home abuse details.

Internet of Things devices should also enact basic principles of security, such as requiring strong passwords and two-factor authentication and logging all users out when the password is reset. In 2019, multiple reports described people hacking into Ring cameras (Hanrahan, 2019), often talking to children (Paul, 2019). And while at least one police department has been trying to help survivors by giving them free Ring devices (Eaton, 2019), survivors should use the product with caution. In 2018, Ring did not log out all parties after a password change, a basic safety precaution given abusers may have the old password and would still have access. This protocol has changed, but a test showed it took several hours to log out all logged-in users (Chang, 2018).

Devices should also have phone numbers to support centers on the device itself and within the app, and customer service representatives should understand the realities of abuse enacted through the device and how to support victims. Companies, while likely unable to fully prevent abuse, are responsible for doing everything possible to prevent abuse and to assist those who do experience abuse through their products.

Given the issues with unwanted "drop in" calls on smart devices, we recommend all two-way communication via smart devices follow the standard model of calls to a cell phone, in which the contact number or name is displayed and the call recipient may accept or decline it. Although many use these devices to monitor their own home or to communicate with friends and family, abuse via these devices must be recognized and planned for.

Domestic violence laws must be updated to include abuse via smart home devices. Police officers, who are often on the front lines of survivor support when responding to domestic violence, should be trained on smart home device abuse. Judges should include the termination of abuse through known and unknown smart home devices in civil no-contact orders. And, a large-scale survey about smart home device abuse is desperately needed.

Stalking

> Erica broke up with John due to his controlling behavior. After the break-up, he began to appear where she was; first at a coffee shop, and then at a restaurant. John was stalking Erica, and though she quickly stopped posting her location on social media and changed the password to any accounts he might have access to, the stalking continued. One day, while driving her Land Rover, the air conditioner turned off. She turned it on, only for it to turn off again. After a few failed attempts, she figured the unit was broken. When she returned to her car after work, all the windows were down, though she knew they were left rolled up. Erica realized John must have control over her car. After a call with Land Rover's customer support, she discovered a second person using the Land Rover app to connect with her car. John accompanied her when she purchased the car, so he knew the registration information needed to connect his app. Without Erica knowing, John knew the car's location at all times, and he had power over the temperature, windows, and could remotely start the car. (Case Study 4)

Before digital automobile interfaces, abusive partners could simply check the odometer of the victim's car to see if they had driven any extra miles (Fazzini, 2018). In the modern age of digitized car controls, abusers have new methods of stalking. Woodlock (2013) found abusers use monitoring technology not just for stalking, but to "create a sense of omnipresence" and to isolate, punish, and humiliate victims (p. 5). The Land Rover InControl app is one example of a product that can be subverted for stalking.

Importantly, while some abusers use spyware to stalk victims, it is more common for them to use legal monitoring apps such as parental control apps, Find My, and theft trackers (Levy, 2018). Designed without intimate partner violence in mind, these apps are weaponized by abusers, often without their victims' knowledge (Levy, 2018). Levy (2018) describes how – for victims of technology-facilitated stalking within a domestic violence context – access credentials such as passwords or security questions are ineffective at keeping an intimate partner out of the victim's accounts. Answers to security questions can often be guessed by an intimate partner, and it may be possible to get someone's passwords via threat of violence. Privacy experts must look beyond the "stranger danger" mentality and create solutions for users whose threat comes from inside the home.

As part of a story on technology-facilitated stalking, a *Wired* magazine writer asked his wife to attempt to secretly monitor his location (Greenberg, 2019b). During his shower, she set up a discrete monitoring method on his phone (Greenberg, 2019b). A popular application sends the user emails summarizing who their location has been shared with, which is a positive step in recognizing possible misuse. However, Greenberg (2019b) noted he did not receive an email the first day. Importantly, the app's creator partnered with domestic violence organizations to modify features that abusers weaponized (Newman, 2017). This practice should be standard across all technology companies.

While many abusers stalk their victims through the use of legitimate apps, others turn to specifically designed "stalkerware" products. In 2018, over 200 apps and services catering to would-be stalkers were identified, with features ranging from location tracking to recovering deleted texts from someone's phone (Valentino-Devries, 2018). Many apps are marketed as tools to monitor children's mobile phone use, but can be exploited. While the desire to keep children safe is understandable, evidence shows invasive snooping does more harm than good (Ghosh, Badillo-Urquiola, Guha, LaViola Jr., & Wisniewski, 2018). Indeed, such apps are an invasion of the child's privacy (Lashbrook, 2019) and may be used by abusive parents to surveil their adult or minor children (Ohlheiser, 2019). For example, SMS Tracker is a child safety product aimed at helping parents. In 2013, a man installed the app on his wife's phone days before murdering her (Valentino-Devries, 2018). Company representatives declined to comment on the app's role in the murder (Valentino-Devries, 2018).

Current law prohibits stalking, but it is not illegal to monitor the location of one's child or install tracking software on one's own phone (Lashbrook, 2019). Most tracking software companies tell users to follow local and federal laws while selling products the purchaser can use to break the law. These companies exist in a legal gray area, and current laws are not placing responsibility on these companies for creating products used for intimate partner stalking.

Eva Galperin, Director of Cyber Security for the Electronic Freedom Foundation, calls stalkerware products "spouseware" because of the high prevalence of people using them to spy on their spouses (Greenberg, 2019a, para 2). She is currently pushing antivirus companies to include stalkerware detection in their products. Galperin hopes that, when a user scans their device for malware or viruses using antivirus software, the program will *also* search for tracking apps (Greenberg, 2019a).

We suggest the following design protocol for GPS-connected apps and services: first, any product with a GPS locator must notify the user when GPS is active, and the product should allow the user to see who has access to the device's location. This information should be immediately visible to the user and not buried within a complex user interface. Moreover, a user should be able to quickly remove unwanted users from having access to their location.

Going Further: The Potential for Intervention within Health, Pregnancy, and Wellness Products

Domestic violence victims feel comfortable using phone technologies compared to other forms of technology (Finn & Atkinson, 2009), and we must meet them where they are. While the authors acknowledge real privacy concerns with fitness and wellness apps, specifically with regard to which companies and entities have access to users' inputted information (Lanzing, 2016; Peppet, 2014), we believe these apps have the potential to identify possible survivors and give meaningful help and support to victims.

> Sandra and Jake had been together for five years when she became pregnant. Jake's physical violence had become a standard part of their relationship. Every few months, something small would set him off. Once, it was Sandra going out with friends after work. Another time, it was finding dirty dishes in the sink. Sometimes, Sandra could calm him down before he attacked, but not always. She was hopeful that it would be different now that she was pregnant, and that having a baby would finally mean an end to the violence she'd endured for years. But, she was wrong. (Case Study 5)

Domestic violence against pregnant women is a serious worldwide problem. In the US, 20% of pregnant women experience domestic violence (Parsons, Goodwin, & Peterson, 2000). The World Health Organization (2011) found physical violence rates against pregnant women ranging from 1% (Japan) to 28% (Peru). In Africa, the rate of physical violence against pregnant partners is 23–40% (World Health Organization, 2011). In America, murder is the leading cause of death for pregnant women, with most assailants being intimate partners (Chang, Berg, Saltzman, & Herndon, 2005).

Given an abuser's goal of maintaining control over their victim, the prevalence of violence during pregnancy is not surprising. Indeed, pregnancy marks a turning point in people's lives, and priorities can change. A pregnant person's increased interest in their baby and sometimes diminished physical and emotional availability to their partner can lead an abuser to attempt to regain control via violence (Campo, 2015).

We believe medical professionals remain the most promising point of intervention for pregnant survivors of domestic violence because most women killed during pregnancy "come into contact with the healthcare system before their deaths" (Frye, 2001). In the age of mobile apps acting as supplementary (or surrogate) medical care, we believe medical, health, and wellness-related apps can be designed to provide help or information to pregnant domestic violence victims.

Thankfully, this type of intervention is already happening in an inadvertent way. The fertility app Glow has reported that users frequently post on the message boards describing abuse and seeking advice (Moscatello, 2017). The use of the message boards as a safe space to ask for help is unsurprising, given that online support spaces are sometimes safer (and less obvious to perpetrators) to utilize than in-person services (Finn & Atkinson, 2009). Moreover, abusers who monitor the victim's online activity often look at browser history (Finn & Atkinson, 2009); a fertility app is a much less obvious place to look (Moscatello, 2017).

While pregnant victims seeking out and receiving advice through fertility message boards is a positive development, pregnancy and health app developers should be intentional about supporting survivors, rather than waiting for them to report abuse. Consideration should be given to how the product could recognize potential abuse and offer support.

Apps should offer users a way to record injuries. If a user records an injury, word recognition from the injury description could trigger an automated response related to domestic violence. This message could say, "This injury could be due to interpersonal conflict. Are you safe? Would you like to see some resources that can help?". App developers can include resources such as the National Domestic Violence hotline number, the addresses and phone numbers of local domestic violence shelters, and a summary of safety planning. The message should encourage the user to write down the information and keep it somewhere the abuser could not find it. Moreover, the survivor should be told to use false names if saving a number in their phone.

A second method of assisting pregnant people experiencing abuse is to have products designed to recognize forced pregnancy. Indeed, 8.6% (10.3 million) of women reported having had an intimate partner who tried to get them pregnant when they did not want to (Black et al., 2011). Many fertility/period tracking apps gather information about the user's reason for using the app, and a user may report they are using the app to avoid pregnancy. Then, if the user reported having unprotected sex (a common feature in fertility apps), the app could ask the user to update their goals or provide information about the encounter. Of course, the user may not want to provide the information or may not be in a safe position to do so. Other options within the app might include reporting that the condom broke, that not using a condom was a mistake, or that their partner refused to wear one. Selecting this last option could trigger a message similar to the injury message, giving the user the option to continue on to a list of local resources. In this case, the list should include local family pregnancy crisis centers. A feature like this could also allow period tracking apps to identify if the user has survived a sexual assault, by providing an option that indicates the sexual encounter was not consensual. The resources listed could include nearby emergency rooms, RAINN's National Sexual Assault Telephone Hotline, and contact information for local sexual assault survivor advocacy groups.

Designers should consider the various reasons a user might decline help. One such concern might be that the button to view resources will take them out of the app and into a browser, which the abuser may monitor. A note next to the "yes" button should clearly state the user will stay within the app. This is merely one consideration. The worst case scenario when designing a feature meant to help survivors is to inadvertently alert the abuser that they are researching domestic violence resources, as this can cause further harm and increased monitoring. Given that the rate of both lethal and non-lethal violence soars when a victim leaves the relationship (McGee, 2005), it is essential designers consider how to best hide when a victim is seeking outside help, services, and/or support.

The Framework for Inclusive Safety

In order to combat digital tools being used for abuse, we suggest technologists use PenzeyMoog's (2020) Framework for Inclusive Safety. The Framework's goal is to help technologists uncover ways their product will be misused, design against such misuse, and uncover possible areas where support or intervention might be offered to the user (Fig. 38.1).

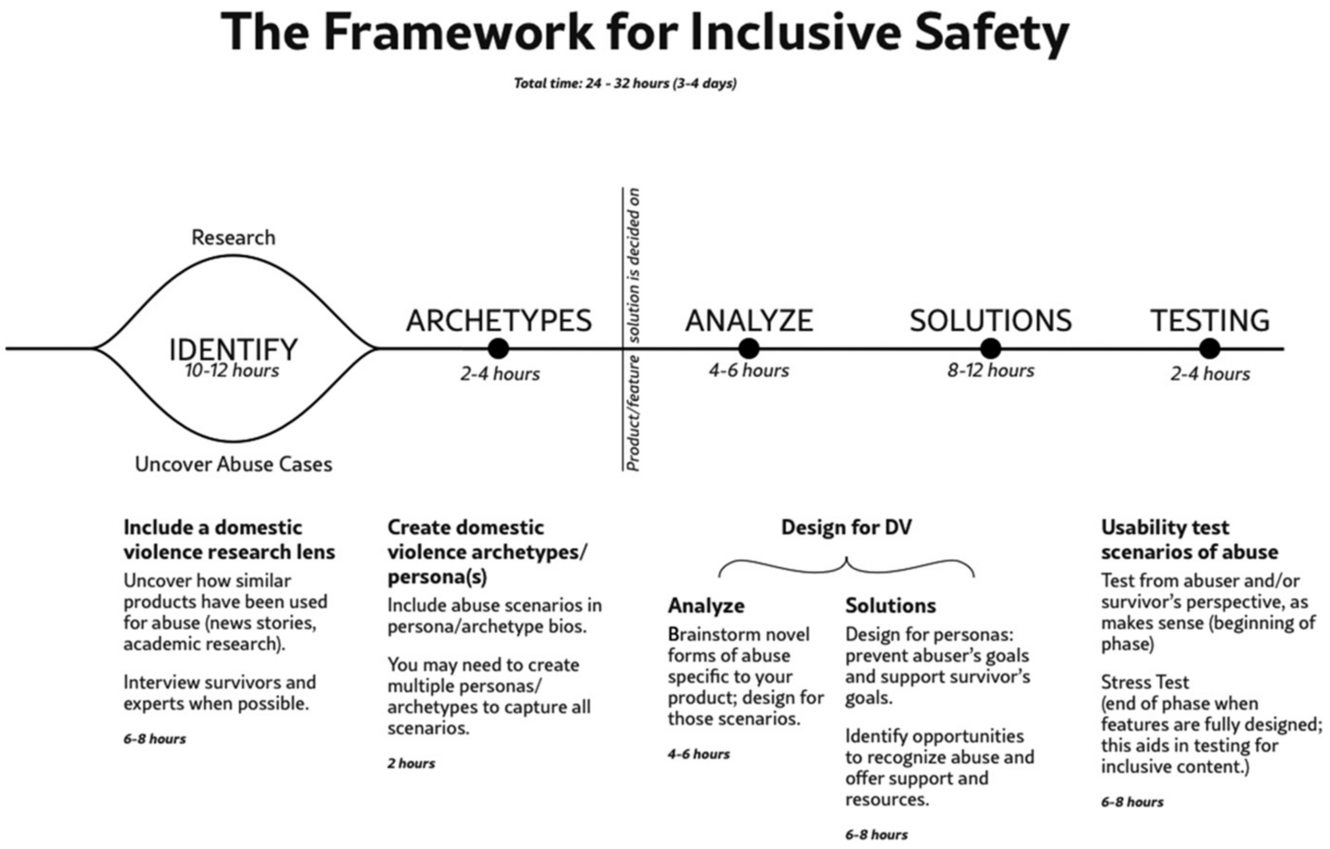
The Framework for Inclusive Safety (PenzeyMoog, 2020):

- Includes a domestic violence research lens.
- Creates domestic violence personas.
- Designs for domestic violence personas.
- Identifies areas where user behavior may indicate abuse and how the product might offer support.
- Includes usability test scenarios and stress testing.

Include Survivors of Domestic Violence in Design Research

Design research leads to better design and safer products. It is critical that developers include domestic violence research within their product ecosystem. First, a developer should research similar products and think critically about safety issues that have already been reported. For example, a team building a smart home device should consider how existing devices are used as abuse tools.

Second, when possible, research should include contact with survivors through surveys and interviews. These surveys or interviews should include a question in which the respondent can describe how the product has been (or could be) used for violence. For example, a team creating a banking app might include a survey question such as, "Can you describe a situation – whether personal or not – in which a financial product has been misused in order to exert financial control?" While more pointed questions are typically best practice for user experience research (the area of design that focuses on users and how they interact with a product), a broadly worded question such as this one gives respondents the freedom to safely respond.



Include a domestic violence research lens

Uncover how similar products have been used for abuse (news stories, academic research).

Interview survivors and experts when possible.

6-8 hours

Create domestic violence archetypes/ persona(s)

Include abuse scenarios in persona/archetype bios.

You may need to create multiple personas/ archetypes to capture all scenarios.

2 hours

Analyze

Brainstorm novel forms of abuse specific to your product; design for those scenarios.

4-6 hours

Solutions

Design for personas: prevent abuser's goals and support survivor's goals.

Identify opportunities to recognize abuse and offer support and resources.

6-8 hours

Usability test scenarios of abuse

Test from abuser and/or survivor's perspective, as makes sense (beginning of phase)

Stress Test (end of phase when features are fully designed; this aids in testing for inclusive content.)

6-8 hours

Fig. 38.1. The Framework for Inclusive Safety within the Design Process. *Source:* Reprinted with Permission from Eva PenzeyMoog.

Create Abuser and Survivor Personas

During research synthesis, designers typically identify the types of people the app or product is targeting and create personas for them. In addition to main archetypes, design teams should create two additional personas: an abuser and a survivor. The abuser persona is someone who can use the product to control, monitor, or harass their victim. The survivor persona is someone who can suffer abuse via the product.

Through this process, the design team may realize a survivor can be secretly surveilled via the product. The next step, then, is for the team to consider *how* a survivor could learn the abuse is happening. Alternatively, the survivor may know surveillance is happening but may not be aware of how to stop it. The design team then needs to consider how a survivor can regain control and power over their app use.

Identify and Design Against Abuse Cases

After research and research synthesis (steps one and two) are complete, the design team should include domestic violence abuse cases within their product design. They should draw upon abuse cases identified in their research and should brainstorm novel abuse cases. The three activities that follow are performed during steps three and four of the design process.

During the third step of the design process, we suggest design teams set aside time for a "Black Mirror Brainstorm" (Lewis, 2018). This term – coined by designer Aaron Lewis (2018) – refers to the hit television series *Black Mirror*, a show in which promising technological advancements harm people. A "Black Mirror Brainstorm" session, then, tasks designers with considering the worst ways their products can be (mis)used.

During the final phase of the design process, when the product is being created (either as a prototype or working technology), the design team should do two types of testing:

(1) *Stress Testing:* Stress testing – a term coined by designers Eric Meyer and Sara Watcher-Boettcher (2016) – is a process by which the design team uses their product through the eyes of someone having an extremely bad day (e.g., someone recently fired from a job). The design team should select a scenario, get into the mindset of someone experiencing a terrible day, and use the product. The design team should identify ways the design makes them feel worse – such as sarcastic text that might make a distressed person feel stupid. Once identified, these designs should be modified.

(2) *Abuse Testing:* Design teams should get into the mindset of an abuser, a survivor, or both, depending on which makes the most sense for the product.

When doing this testing, best practice is to find real people who fit the characteristics, have them use the design, and give feedback. However, the ethics of finding someone experiencing their worst day and asking them to test your product are questionable. Similarly, it would be difficult to find a domestic abuser who would willingly product test and discuss how the product facilitates abuse. In these cases, it is acceptable for the design team to role-play and do the testing themselves. However, we do not recommend this approach for other attempts at inclusive design; for example, it would be inappropriate for a white designer to attempt to be in the mindset of Black user to ensure a product is racially inclusive. In this case, the team should hire members of those groups to do testing.

Identify Areas Where User Behavior May Indicate Abuse and How the Product Might Offer Support

If designed properly, financial products, as well as health, wellness, and pregnancy products, could help identify abusive behavior. The design team should conduct a full audit of the product's features and brainstorm what user behavior might indicate abuse. Moreover, they should discuss what resources would be most appropriate to include within the product if a user indicates abuse. Designers should also consider the user's level of safety if the product includes domestic violence resources.

A Final Note on the Importance of Diverse and Inclusive Teams

The importance of diverse, inclusive teams within technology companies is well-documented. Diversity can foster creativity, improve performance, help innovation (Diversity in Tech, 2020; Forbes Technology Council, 2018), and promote empathy (Walter, 2016). Indeed, it is important for technologists to be able to empathize with minority people who are discriminated against by other product users (e.g., when a white Airbnb host refuses to accept a booking from a Black user, as described by Romano, 2016). When people from multiple minority groups belong to a team, there is more open communication about product misuse.

Conclusion

Differences in social location, race, class, (dis)ability status, and the like can produce differential victim experiences with intimate partner violence. Although the scope of this chapter precluded us from an in-depth discussion of intersectionality, the authors want to acknowledge that the intersectional identities of survivors (e.g., their class, race, location, etc.) should also be identified and included during the design process. During the research phase of *any* product, designers should identify who their users are (along multiple dimensions). What designers learn about their users during the research phase should then be utilized during the ideation portion of the design process, with a goal of making the product work for all users.

Within the context of designing against domestic violence, it is imperative that women, who are disproportionately likely to be abuse survivors, are part of the teams creating digital products. However, survivors should *not* be expected to do the emotional work of convincing colleagues as domestic violence is a deadly, common occurrence. Workplace training about technology-based domestic violence can help all colleagues see the importance of designing against domestic violence.

Technology is used to perpetuate domestic abuse (George & Harris, 2014; Woodlock, 2013) and is another mechanism by which abusers exert control and dominance over victims. As described in this chapter, technology can be used by abusers to financially control, stalk, or gaslight victims. Given the role of technology in abuse, coercive control, and stalking, it is vital that designers consider domestic violence when creating new technologies. The Framework for Inclusive Safety (PenzeyMoog, 2020) provides technologists with actionable steps toward making products safer.

While technology is undoubtedly used in ways that are harmful toward victims, technology can also serve as a safe place for victims to receive discreet help and assistance (Finn & Atkinson, 2009). As described in this chapter, we believe health, pregnancy, and wellness products can be designed to provide helpful resources in a safe manner. Ultimately, we recognize the limitations of single solutions used in isolation to stop domestic violence and encourage designers to use multiple techniques in order to ensure digital products are as safe and inclusive as possible. The framework detailed in this chapter provides a starting point.

References

Allen, J. V. (2000). Financial abuse of elders and dependent adults: The FAST (Financial Abuse Specialist Team) approach. *Journal of Elder Abuse & Neglect*, *12*(2), 85–91.

Australia. (1975). Family Law Act 1975 (Cth).

Becky's Fund. (n.d.). Coerced debt. Retrieved from https://beckysfund.org/resources/coerced-debt/

Belknap, J., & Melton, H. (2005). Are heterosexual men also victims of intimate partner abuse? *VAWnet.org: The National Online Resource Center for Violence Against Women*. Retrieved from https://vawnet.org/sites/default/files/materials/files/2016-09/AR_MaleVictims.pdf

Black, M. C., Basile, K. C., Breiding, M. J., Smith, S. G., Walters, M. L., Merrick, M. T., & Stevens, M. R. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 summary report. *Centers for Disease Control and Prevention*. Retrieved from https://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf

Bowles, N. (2018, June 23). Thermostats, locks and lights: Digital tools of domestic abuse. *The New York Times*. Retrieved from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Campo, M. (2015). Domestic and family violence in pregnancy and early parenthood. *The Australian Institute of Family Studies*. Retrieved from https://aifs.gov.au/cfca/publications/domestic-and-family-violence-pregnancy-and-early-parenthood

Chang, L. (2018, May 14). A Ring doorbell vulnerability lets people snoop even after a password change. Retrieved from https://www.digitaltrends.com/home/ring-video-doorbell-security-exploit/

Chang, J., Berg, C. J., Saltzman, L. E., & Herndon, J. (2005). Homicide: A leading cause of injury deaths among pregnant and postpartum women in the United States, 1991–1999. *American Journal of Public Health*, *95*(3), 471–477.

Chesterman, J. (2015). Taking control: Putting older people at the centre of elder abuse response strategies. *Australian Social Work*, *69*(1), 115–124.

Commonwealth Bank of Australia. (2020). Domestic & family violence assistance. Retrieved from https://www.commbank.com.au/support/dv-assistance.html

Diversity in Tech. (2020). The benefits of diversity in tech. Retrieved from https://www.diversityintech.co.uk/the-benefits-of-diversity-in-tech

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, *59*, 551–570.

Eaton, E. (2019, December 29). San Antonio domestic violence victims receive free Ring surveillance devices from local police agencies. *San Antonio Express-News*. Retrieved from https://www.expressnews.com/news/local/article/San-Antonio-domestic-violence-victims-receive-14932616.php

Fazzini, K. (2018, November 5). Secret apps and self-'doxing': How victims of domestic abuse are escaping tech-savvy abusers. *CNBC*. Retrieved from https://www.cnbc.com/2018/11/05/victims-of-domestic-violence-challenged-by-abusers-using-technology.html

Financial Crime Enforcement Network. (2011). Advisory to financial institutions on filing suspicious activity reports regarding elder financial exploitation. Retrieved from https://www.fincen.gov/sites/default/files/advisory/fin-2011-a003.pdf

Finn, J., & Atkinson, T. (2009). Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the Technology Safety Project. *Journal of Family Violence*, *24*, 53–59.

Forbes Technology Council. (2018). 12 Ways Diversity Makes A Difference In Tech. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/12/12-ways-diversity-makes-a-difference-in-tech/#50991c362bc6

Frye, V. (2001). Editorial: Examining homicide's contribution to pregnancy-associated deaths. *Journal of the American Medical Association: The Journal of the American Medical Association*, *285*(11), 1510–1511.

George, A., & Harris, B. (2014). *Landscapes of violence: Women surviving family violence in regional and rural Victoria*. Melbourne, VIC: Deakin University. Retrieved from https://www.deakin.edu.au/__data/assets/pdf_file/0003/287040/Landscapes-of-Violence-online-pdfversion.pdf

Ghosh, A. K., Badillo-Urquiola, K., Guha, S., LaViola, J. J., Jr., & Wisniewski, P. J. (2018). Safety vs. surveillance: What children have to say about mobile apps for parental control. In *Proceedings of the 2018 CHI conference on human factors in computing systems [Paper No. 124]*. doi:10.1145/3173574.3173698

GovTrack. (2007). S. 1136 (110th): Survivors' Empowerment and Economic Security Act. Retrieved from https://www.govtrack.us/congress/bills/110/s1136

Graham, J. (2019, May 14). Alexa Guard can now listen for alarms – or, perhaps, a cheating spouse? *USA Today*. Retrieved from https://www.usatoday.com/story/tech/talkingtech/2019/05/14/alexas-latest-skill-listening-alarms-and-snooping-home-life/1189230001/

Greenberg, A. (2019a, April 3). Hacker Eva Galperin has a plan to eradicate stalkerware. *Wired*. Retrieved from https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

Greenberg, A. (2019b, July 2). The simple way Apple and Google let domestic abusers stalk victims. *Wired*. Retrieved from https://www.wired.com/story/common-apps-domestic-abusers-stalk-victims/

Hanrahan, M. (2019, December 12). Ring security camera hacks see homeowners subjected to racial abuse, ransom demands. *ABC News*. Retrieved from https://abcnews.go.com/US/ring-security-camera-hacks-homeowners-subjected-racial-abuse/story?id=67679790

Harris, B. (2018). Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice. In K. Fitz-Gibbon, S. Walklate, J. McCulloch, & J. Maher (Eds.), *Intimate partner violence, risk and security: Securing women's lives in a global world* (pp. 52–70). London: Routledge.

Hunter, R. (2006). Narratives of domestic violence. *Sydney Law Review*, *28*(4), 733.

Kippert, A. (2019). Smart home technology is being used against survivors. Retrieved from https://www.domesticshelters.org/articles/technology/smart-home-technology-is-being-used-against-survivors

Lanzing, M. (2016). The transparent self. *Ethics and Information Technology*, *18*, 9–16.

Lashbrook, A. (2019, September 18). The case against spying on your kids with apps. *OneZero*. Retrieved from https://onezero.medium.com/the-case-against-spying-on-your-kids-with-apps-59760ec780e0

Levy, K. (2018, March 1). No safe haven for victims of digital abuse. *Slate*. Retrieved from https://slate.com/technology/2018/03/apps-cant-stop-exes-who-use-technology-for-stalking.html

Lewis, A. (2018, November 16). In light of the latest FB scandal, here's my proposal for replacing Design Sprints: Black Mirror Brainstorms. A workshop in which you create a Black Mirror episode. The plot must revolve around misuse of your team's product. Pair with @brownorama's idea of "abusability testing" [Tweet]. Retrieved from https://twitter.com/aaronzlewis/status/1063544871472914432

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011). College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking*, *14*, 711–716.

McFarlane, J., Campbell, J. C., & Watson, K. (2002). Intimate partner stalking and femicide: Urgent implications for women's safety. *Behavioral Sciences and the Law*, *20*, 51–68.

McGee, S. G. S. (2005). 20 Reasons why she stays: A guide for those who want to help battered women. Retrieved from http://stopviolence.com/domviol/WhySheSometimesStays.pdf

Meyer, E. (2020). Compassionate design. Retrieved from https://vimeo.com/201986969

Meyer, E. A., & Wachter-Boettcher, S. (2016). *Design for real life*. New York, NY: A Book Apart.

Morton, H. (2018). Combatting elder financial exploitation. *National Conference of State Legislatures*, *26*(20). Retrieved from https://www.ncsl.org/research/financial-services-and-commerce/combatting-elder-financial-exploitation.aspx

Moscatello, C. (2017, September 5). The disturbing conversations women are having on fertility apps. *Elle*. Retrieved from https://www.elle.com/life-love/a12138580/the-disturbing-conversations-women-are-having-on-fertility-apps/

National Australia Bank Limited. (2020). Domestic and family violence support. Retrieved from https://www.nab.com.au/about-us/social-impact/customers/domestic-and-family-violence

National Network to End Domestic Violence. (2014). Join NNEDV & the Allstate Foundation as we say 'no more' to financial abuse this April. Retrieved from https://nnedv.org/latest_update/join-nnedv-the-allstate-foundation-as-we-say-no-more-to-financial-abuse-this-april/

Newman, L. H. (2017, February 1). Tech can do more to help survivors of abuse. Here's where to start. *Wired*. Retrieved from https://www.wired.com/2017/02/tech-can-help-survivors-abuse-heres-start/

Ohlheiser, A. (2019, Oct. 22). 'Don't leave campus': Parents are now using tracking apps to watch their kids at college. *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2019/10/22/dont-leave-campus-parents-are-now-using-tracking-apps-watch-their-kids-college/

Parsons, L., Goodwin, M. M., & Peterson, R. (2000). Violence against women and reproductive health: Toward defining a role for reproductive health care services. *Maternal and Child Health Journal*, *4*(2), 135–140.

Paul, K. (2019, December 27). Ring sued by man who claims camera was hacked and used to harass his kids. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/dec/27/ring-camera-lawsuit-hackers-alabama

PenzeyMoog, E. (2020). The framework for inclusive safety. Retrieved from www.inclusivesafety.com

Peppet, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review*, *93*(1), 85–179.

Petrosky, E., Blair, J. M., Betz, J., Fowler, K. A., Jack, S. P. D., & Lyons, B. H. (2017). Racial and ethnic differences in homicides of adult women and the role of intimate partner violence—United States, 2003–2014. *Morbidity and Mortality Weekly Report*, *66*(28), 741–746. Retrieved from https://www.cdc.gov/mmwr/volumes/66/wr/pdfs/mm6628a1.pdf

Postmus, J. L., Plummer, S.-B., McMahon, S., Murshid, N. S., & Kim, M. S. (2012). Understanding economic abuse in the lives of survivors. *Journal of Interpersonal Violence*, *27*, 411–430. doi:10.1177/0886260511421669

Queensland Domestic and Family Violence Death Review and Advisory Board. (2017). Queensland Domestic and Family Violence Death Review and Advisory Board 2016–17 Annual Report. Retrieved from https://www.courts.qld.gov.au/__data/assets/pdf_file/0003/541947/domestic-and-family-violence-death-review-and-advisory-board-annual-report-2016-17.pdf

Robertson, K., & Murachver, T. (2011). Women's and men's use of coercive control in intimate partner violence. *Violence & Victims*, *26*, 208–217.

Romano, A. (2016, May 6). Airbnb has a discrimination problem. Ask anyone who's tried to #Airbnbwhileblack. *Vox*. Retrieved from https://www.vox.com/2016/5/6/11601180/airbnbwhileblack-racism

S. 627: SAFE Act of 2019. (2019). GovTrack. Retrieved from https://www.govtrack.us/congress/bills/116/s627. Accessed on April 2020.

Sharp-Jeffs, N. (2015). A review of research and policy on financial abuse within intimate partner relationships. *Child and Woman Abuse Studies Unit (CWASU)*. Retrieved from https://cwasu.org/wp-content/uploads/2015/12/Review-of-Research-and-Policy-on-Financial-Abuse.pdf

Stark, E. (2006). Commentary on Johnson's "conflict and control": Gender symmetry and asymmetry in domestic violence. *Violence Against Women*, *12*, 1019–1025.

Stark, E. (2007). *Coercive control: How men entrap women in personal life*. New York, NY: Oxford University Press.

Stark, C. A. (2019). Gaslighting, misogyny, and psychological oppression. *The Monist*, *102*, 221–235.

Statista. (2020). Smart home. Retrieved from https://www.statista.com/outlook/279/109/smart-home/united-states

Stetson Law (n.d.). Mandatory reporting statutes for elder abuse, 2016. Retrieved from https://www.stetson.edu/law/academics/elder/home/media/Mandatory-reporting-Statutes-for-elder-abuse-2016.pdf

Sweet, P. L. (2019). The sociology of gaslighting. *American Sociological Review*, *84*(5), 851–875.

United Nations Office on Drugs and Crime. (2018). Global study on homicide - Gender-related killing of women and girls. Retrieved from https://www.unodc.org/documents/data-and-analysis/GSH2018/GSH18_Gender-related_killing_of_women_and_girls.pdf

United States Department of Justice. (n.d.a). Domestic violence. Retrieved from https://www.justice.gov/ovw/domestic-violence

United States Department of Justice. (n.d.b). State elder abuse statutes. Retrieved from https://www.justice.gov/elderjustice/elder-justice-statutes-0

Valentino-Devries, J. (2018, May 19). Hundreds of apps can empower stalkers to track their victims. *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html

Walter, J. (2016, June 6). Diversity in Tech: The unspoken empathy gap. *Medium*. Retrieved from https://medium.com/tech-diversity-files/diversity-in-tech-the-unspoken-empathy-gap-5b806c83d717

Woodlock, D. (2013). Technology-facilitated stalking: Findings and recommendations from the SmartSafe project. *Domestic Violence Resource Centre*. Retrieved from http://www.dvrcv.org.au/sites/default/files/SmartSafe_0.pdf

World Health Organization. (2011). Intimate partner violence during pregnancy. Retrieved from https://apps.who.int/iris/bitstream/handle/10665/70764/WHO_RHR_11.35_eng.pdf;jsessionid=792A222F6375EF41029EC817F8C9D25F?sequence=1

World Health Organization. (2017). Violence against women. Retrieved from https://www.who.int/news-room/fact-sheets/detail/violence-against-women