Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse

Tara Matthews, Kathleen O’Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, and Martin Shelton | Google
Cori Manthorne | CORA (Community Overcoming Relationship Abuse)
Elizabeth F. Churchill and Sunny Consolvo | Google

Survivors of intimate partner abuse (IPA) are people who’ve experienced emotional abuse, threats of physical or sexual violence, or actual physical or sexual violence from an intimate partner—typically a current or former spouse, spouse during the process of separating, or dating partner. Approximately one in four women and one in 10 men in the US have experienced negative impacts from sexual violence, physical violence, or stalking by an intimate partner; approximately one in three women worldwide have experienced physical or sexual violence by an intimate partner. Because IPA affects so many people globally, the survivors and abusers vary in gender, culture, wealth, education, tech literacy, and other attributes.

Survivors of IPA would greatly benefit from a technology community that understands and continues to address their unique challenges. To help technology creators better support survivors of IPA, we share findings from a study aimed at understanding this population’s digital privacy and security experiences and practices. Our study builds on prior research outlining different phases of IPA (for example, Lenore Walker’s three phases of abuse and Shirley Patton’s five phases of leaving). We also draw on research focused on improving the usability of general online privacy and security technologies (for example, Lorrie Cranor and Simson Garfinkel’s work). We believe that understanding the experiences of survivors of IPA can improve digital privacy and security for the general population.

Formative Study
Our study sought to answer the following research questions:

- How do survivors of IPA experience digital privacy and security?
- What are survivors’ motivations, practices, and challenges when protecting their privacy and security online and on their devices?

To this end, we conducted one-hour semistructured interviews with 15 survivors of IPA (14 female, one male). All participants were of low socioeconomic status, receiving services from two US nonprofit agencies. We worked with agency staff to co-create a study plan. Agency staff recruited participants who were at least 18 years of age and had a digital privacy or security
concern, such as experiencing an account breach. For more information about our study’s methodology, please see “Stories from Survivors: Privacy and Security Practices When Coping with Intimate Partner Abuse.”

Ethical Considerations
This research entailed important ethical considerations. Throughout the process, we referred to pre-existing literature and consulted with more than a dozen experts in domains including survivors of IPA, human subjects research, legal, ethics, security, privacy, and anonymization.

Participant well-being shaped our study design. Our agency collaborators recruited using our criteria so that participants wouldn’t need to communicate with us until they decided to participate. We conducted interviews at the agencies to help participants feel more comfortable. Our interviews focused on technology-related abuse, not general stories of abuse unrelated to technology. We also made aftercare arrangements to communicate with the agencies if anything problematic came up during interviews.

We anonymized the data we report following the guidance of multiple privacy experts and agency collaborators. Also, our findings focus on informing the technology community. We assessed prior literature and confirmed that our findings organized known abuser attacks and survivor practices into a framework with corresponding recommendations for technology designers. We describe additional ethical considerations in “Stories from Survivors: Privacy and Security Practices When Coping with Intimate Partner Abuse.”

Three IPA Phases Affecting Technology Use
We observed three phases of IPA—physical control, escape, and life apart (see Figure 1)—that affected how survivors used technology, focusing on their digital privacy and security practices. This framework gives technology creators a lens through which to consider how survivors of IPA might experience or leverage new and existing technologies. Note that this framework describes how survivors’ experiences and use of technology are likely to change across the different phases.

Physical Control
He’s really controlling, and he doesn’t want me to even have anything online. … Like, he wants me to be alone and have nobody. So I could just call him whenever I need him, just so he’s the only one.
—Participant (P) 12

Participants first faced the physical control phase, during which their abuser had regular physical access to them and their devices. Abusers used this physical proximity to control and monitor participants’ devices and accounts. Although some participants found ways to use technology rather than avoid it completely, all described challenges maintaining autonomy and privacy while using technology because of their abusive relationships. For multiple participants, the abuser’s physical control of their technology contributed to social isolation, device loss or damage, financial hardship, and psychological distress.

Survivor experiences. During the physical control phase, abusers violated participants’ digital privacy and security by

- physically controlling and monitoring their devices and accounts,
- destroying their devices, and
- installing spyware on their devices.

Abusers also hijacked participants’ accounts and harassed them online during the physical control phase. Such hijacking also occurred during the other two phases.

P3 explained how her abuser monitored her digital activity by forcing her to give him physical access to her phone. She said: “When we were together, he would always have my phone. Whoever would text me, he had to see who it was first. Or who was calling me, he had to check to make sure it wasn’t another guy.”

P4’s abuser had destroyed several of her phones. She told us “he would
just, like, stomp on it.” This isolated her from her social relations. In her words, “people have my old numbers … there was no way for me to get a hold of other people.” P4 had to deal with being phoneless for some time due to the difficulty of purchasing a new phone in her situation.

P2 observed unusual behavior on her phone and, with help from an expert at a store, found spyware. She explained that the expert told her that “somebody put something in the phone … [so that they] can see … where you call, who you talk to, all the logs …”

Participants experienced threats online in all three phases. For example, P4 described: “He would just talk about me with my name, my family’s name … all this information, he would just put it on [the social network]. … Because he was basically being a bully, as well, through [the] Internet, saying he was gonna kill me, kill my mom, kill my dad, kill my [siblings].”

Account hijacking was another abuser attack that participants experienced in all three phases. For example, P7’s abuser hijacked her email account and impersonated her. He also deleted emails about potential jobs for her. She told us: “He read personal emails and responded to personal emails in my voice. And he deleted job information.” She found it to be “rather personal and damaging.”

Survivor practices. To cope with their abusers’ physical control of their devices and accounts, participants reported

- limiting or avoiding use of devices and accounts their abusers could access,
- using alternate devices and accounts their abusers didn’t know about, and
- deleting material from their devices and accounts (such as messages and browsing histories).

For example, after P2 found spyware on her phone and laptop, she said: “I simply stopped using the laptop at home. And the phone. That’s why I went to the library to use the computer.”

Escape

I was trying to figure out a way to get out. And so I was moving stuff out of our house a little at a time while he was at work. … I got that little prepaid phone and then I called from there. … I was just in the middle of the street. —P11

During the escape phase, participants’ main goal was to leave and sever ties with their abuser. The escape phase overlapped with the other two phases, so it inherited the same abuser attacks and survivor practices as those phases. However, it added new privacy and security challenges due to the survivors’ life circumstances. The National Domestic Violence Hotline estimates that it takes an average of seven attempts to succeed.7 Research shows that abusers escalate their attempts to regain control over survivors during this time, resulting in an increased likelihood of violence and even death.7 Thus, in Figure 1, we mark escape as being an acute risk and depict the phases as a cycle.

Survivor practices: escape during physical control. During the physical control portion of the escape phase, participants focused on hiding their digital escape activities, for example, learning how to escape, setting up social support, and finding new housing and jobs. They used the same practices described for the physical control phase, but possibly more often because, as noted, abusers might escalate their efforts.

As an example of escape during physical control, P8 told us how she used an alternate account on her work computer: “I was trying to look for elsewhere to live and trying to find resources out there and trying to apply to, you know, just housing and things like that. And I didn’t want it to go to where he would find it. So … I’d go into [my separate email account] at work only, I didn’t want [that account] on my phone or anything.”

As another example of escape during physical control, P2 explained how she deleted her browsing history from her home computer to hide some of her search activities from her abuser and her child: “[I delete my browsing history because] my [child] sometimes [uses] the computer; I don’t want [my child] to know that I am like searching how to get a restraining order, … how to kick my husband out of the house. How to help my [child] cope with separate parents, how to help your [child] in school with those kind of issues. … But I don’t want [my child] to see what I am searching; [my child] will start asking questions and I am not ready.”

Survivor practices: escape during life apart. During the life apart portion of escape, participants needed to sever digital ties with their abusers. To do so, participants

- deactivated or abandoned accounts known to the abuser;
- destroyed, discarded, or wiped devices; and
- strengthened authentication.

After leaving, P3 deactivated her social media account in an effort to hide her new location. She suspected her abuser had located her through the account during a previous escape attempt, saying “he’d find so many ways to find out where I was.” The decision to deactivate an account often involved balancing digital privacy and security with access to social support, both of which were important during escape and
life apart. After deactivating her social media account, P3 risked reactivating it to contact her mother: “My mom didn’t have a phone back then. So I had to … use the [social media account] to talk to her. So it was scary.”

P6, whose abuser had installed spyware on her phone, didn’t trust that a reset would completely fix the problem. So after leaving her abuser, she destroyed her phone, saying: “Bye-bye phone. SIM card through the shredder. … The phone unit, painstakingly ran over by a car a couple of times. I mean, it’s in pieces.”

Several participants decided to keep their online accounts, but reported strengthening how they authenticated. P11 recalled: “[A software product] let me know when someone’s trying to hack into my account. Then I used the [two-factor authentication] method, and I changed the password. So that is so cool for me. It’s a couple times. I think the last time was my ex. You know he thought he could just check my email and see what I’m doing.”

Life Apart

I had given up my home, left my job, relocated to another county and not this one that we’re sitting in. My [children] had to go through this. … I had spent a lot of money, lost a lot of money, and had gone through a lot of tech devices. —P6

During the life apart phase, participants described having to start over—often with a new home, job, schools for their children, devices, and accounts—while also dealing with the immediate and long-term risk of their abuser finding information about them. After severing digital ties as part of escape, participants had lifelong privacy work to do, ensuring that they, their children, and other people took great care when sharing their personal information online.

Survivor practices. Participants exerted special care to protect their location (anywhere they or their family go) and contact information (new email addresses, phone numbers, online identities, and so on). They did this to prevent abusers from harassing them or reestablishing physical control. To protect their personal information, participants

- limited or avoided sharing information online,
- monitored and restricted their children’s online activities,
- strengthened the privacy and security settings for their online accounts, and
- severed ties with social relations they had in common with their abuser.

Several participants reported limiting or avoiding sharing information online. But this limited job opportunities for some, as described by P15, who was self-employed but could no longer advertise her services and thus had to change careers: “I have my [small business], but when I was actively working, so you have your email on [the advertisement]. And then you have your phone number. You [include] when you’re going to [be there]. … They know right where to find you, and sometimes, you’re there by yourself. You’re just a sitting duck.”

An important challenge in staying hidden was that the abuser could use other people—such as the participant’s children, family, friends, and colleagues—to find the participant. This concern greatly complicated participants’ online privacy and security work, because it required them to enlist the cooperation of other people who might not fully understand or appreciate their situation. For example, P11 told us that she doesn’t allow her teenager to post on social media. She said, “I just don’t want [my teenager] posting something out there that could be threatening to [him/her] or to our entire family, [he/she] doesn’t even realize it. Like if [he/she] puts … where you go to school. … That means [my abuser] could be sitting outside waiting in the carpool lane, or in the morning when they get to school, there he is.”

Some participants decided to sever ties with social relations they shared with their abuser. For example, P5 said: “I’ve gotten rid of a lot of friends. … They’re mutual friends [with the abuser]. … People can flip-flop, play one side, or [talk] to me and then go give him information. I just don’t trust anybody.”

What’s Working and What Can the Tech Community Do Next?

Our study highlights ways in which technology is already working well for survivors across the three IPA phases that affect technology use. It also highlights opportunities for technology creators seeking to support survivors of IPA.

Using Controls to Delete or Hide Online Activities in High-Stress Situations

Deleting or hiding online activities such as messages and browsing was an important strategy for survivors in all phases, especially physical control. Fortunately, there are already ways survivors can do this; for example, many technologies allow users to have more than one account or device, access multiple accounts on a device, and delete content.

However, as noted, participants in our study reported occasionally making mistakes when deleting or clearing information, perhaps due to the high levels of stress and risk they were facing. Future work could make further improvements by studying such tools’ usability during high-stress, high-risk situations.
Educating Survivors about Security Features

Account hijacking was an issue our participants dealt with in all phases. For those who knew how to use them, security features and controls like two-factor authentication and unusual activity alerts were very empowering, particularly in the life apart phase. However, confidence using these features, especially in high-risk situations, was an issue. Future work could focus on providing instructional materials for survivors and their service providers about how to use privacy and security features and controls.

Managing Digital Evidence of Abuse

It might come as a surprise, but there was an upside to some of the harassing messages that participants received from their abusers—these messages were sometimes provided as evidence to law enforcement (for example, to help obtain restraining orders). Prior work has also shown that digital channels can provide an outlet for an abusers’ desire to exert control, which might reduce their motivation to exert control in other ways.7

However, survivors tend to experience emotional trauma as a result of such harassment. Future work could explore solutions that capture digital evidence and provide abusers with an outlet while minimizing survivors’ emotional trauma.

Maintaining Online Social Lives

Some participants chose to avoid technology to limit the information an abuser could find about them online; however, this also socially isolated them at a time when they needed support and access to resources such as housing and jobs. Several practices commonly used by our participants—avoiding technology, deactivating accounts, and destroying devices—added to their social isolation. Future work could educate survivors about existing technologies and explore new technological solutions to help them maintain social ties without leaking important personal information.

Providing Options and Ambiguity

Survivors must deal with highly motivated attackers who have intimate knowledge of their lives. In the physical control phase, attackers also have physical access to the survivors’ devices and accounts. There is no one-size-fits-all solution to this type of threat. To cope, survivors benefit from having multiple privacy and security options to deal with their highly individual situations. In addition to the features we discussed, survivors benefit from the ability to maintain ambiguity in their technology-mediated interactions with others.10 One way to do this is to give them the space to tell stories about those interactions. For example, survivors could explain that they missed a call from their abuser by claiming that they didn’t hear the call (for example, by saying that their phone ringer was off or they left their phone behind). Another way to give survivors space is to provide granular controls such as the ability to delete specific content, ignore messages, or temporarily turn features off; such controls can also help users manage this type of ambiguity.

We shared results from a formative study on the digital privacy and security experiences and practices of survivors of IPA. Our aim is to help technology creators consider how new and existing technologies and features can be designed to help survivors of IPA as well as identify opportunities to continue to improve support for this user population.

Acknowledgments

This article summarizes a paper previously published in the proceedings of the 2017 SIGCHI Conference on Human Factors in Computing Systems.3 We thank Ali Lange, Allison Woodruff, Ben Petskosky, Clara Sherley-Appel, Elie Burzstein, Erin Simon, Heather Lipford, James Tarquin, Jessica Staddon, Keith Enright, Lawrence You, Lea Kissner, Matt Moore, Michael Falgoust, Michael Janosko, Parisa Tabriz, Patrick McDonald, and Thomas Roessler for their support, feedback, and ideas regarding this research and article. We thank our many colleagues at Google and our collaborators from the agencies for their fantastic support and ideas as we planned and conducted this research. We thank our reviewers and other members of the HCI and usable privacy and security communities who provided input along the way. Most importantly, we thank our participants for their willingness to share their stories, and for their courage.

References


Tara Matthews is a user experience researcher at Google. Contact her at taramatthews@google.com.

Kathleen O’Leary is a PhD student at the University of Washington. She performed this work while a user experience research intern at Google. Contact her at katieole@gmail.com.

Anna Turner is a user experience researcher at Google. Contact her at annaturn@google.com.

Manya Sleeper is a user experience researcher at Google. Contact her at manya@google.com.

Jill Palzkill Woelfer is a user experience researcher at Google. Contact her at jillwoelfer@google.com.

Martin Shelton is a user experience researcher at Google. Contact him at martinskelton@google.com.

Cori Manthorne is a director of programs at CORA (Community Overcoming Relationship Abuse). Contact her at corim@corasupport.org.

Elizabeth F. Churchill is a director of user experience at Google. Contact her at churchill@acm.org.

Sunny Consolvo is a user experience researcher at Google. Contact her at sconsolvo@google.com.