Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse

Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne*, Elizabeth F. Churchill, Sunny Consolvo
Google, Mountain View, CA, USA,
taramatthews@google.com, katieole@gmail.com, {annaturn, manya, jillwoelfer, martinshelton}@google.com, churchill@acm.org, sconsolvo@google.com
*Community Overcoming Relationship Abuse, San Mateo, CA, USA
corim@corasupport.org

ABSTRACT
We present a qualitative study of the digital privacy and security motivations, practices, and challenges of survivors of intimate partner abuse (IPA). This paper provides a framework for organizing survivors' technology practices and challenges into three phases: *physical control*, *escape*, and *life apart*. This three-phase framework combines technology practices with three phases of abuse to provide an empirically sound method for technology creators to consider how survivors of IPA can leverage new and existing technologies. Overall, our results suggest that the usability of and control over privacy and security functions should be or continue to be high priorities for technology creators seeking ways to better support survivors of IPA.

Author Keywords
Privacy; security; user study; intimate partner abuse; domestic violence.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION

With the prominence and pervasiveness of technology in our lives, technology users have reason to attend to their digital privacy and security. Much personal information is collected and stored in online accounts: location in order to power navigation or fitness apps, photos on social media, personal communications in messaging and email apps, and so on. Privacy and security features can help protect users' data from malicious third parties. But for many technology users, the potential actions of an ill-intentioned third party seem an unlikely concern.

CHI 2017, May 06-11, 2017, Denver, CO, USA
ACM 978-1-4503-4655-9/17/05.
http://dx.doi.org/10.1145/3025453.3025875

Some technology users, however, may already be specifically targeted by ill-intentioned third parties. These user populations may include survivors of abuse or human trafficking, political activists, online celebrities, displaced persons, people of low socioeconomic status, and so on. Such users may be specifically targeted because of what they do, who they are, where they are, or who they are with.

While considerable research has focused on digital privacy and security for the majority of users, less has focused on users who, as a result of their particular life circumstances, may be specific targets of ill-intentioned third parties. Understanding the unique digital privacy and security experiences and challenges of such user populations is important for designers who wish to help them better navigate and deploy privacy and security controls online and on their devices. Furthermore, understanding the unique challenges of specific populations can help designers improve technology for both that specific population and the broader population [17].

We present a study of the digital privacy and security motivations, practices, and challenges of a specific population facing higher levels of risk in their daily lives: survivors of intimate partner abuse (IPA). These are people who are broadly targeted by an intimate partner, typically a current or former significant other or dating partner. They may experience threats or actual abuse from their abuser, including sexual, physical, and psychological abuse; stalking; and control of reproductive or sexual health [6]. They may also be controlled financially or spiritually. The abuse can be one-way or mutual and it can take place along a continuum from a single incident to ongoing abuse [6]. Survivors of IPA have a persistent attacker, who has intimate knowledge of their lives. When they share custody of children, a survivor may be legally bound to maintain contact with their persistent attacker, even if they no longer live together.

IPA is common: an estimated 27.3% of women and 11.5% of men in the U.S. have experienced negative impacts from sexual violence, physical violence, or stalking by an intimate partner [6]; about 30% of women worldwide who have been in a relationship have experienced physical or

sexual violence by an intimate partner [44]. The U.S. Centers for Disease Control and Prevention estimates that in the U.S., nearly 27 million women and nearly 16 million men have experienced severe physical violence by an intimate partner at some point in their lifetime [6]. Because IPA affects so many people across the U.S. and the world, survivors and abusers may vary in gender, culture, wealth, education, tech literacy, and other attributes. Survivors of IPA would likely benefit from designers and technologists who understand their specific digital privacy and security needs. In our study, we focused on women and men living in the U.S., of low socioeconomic (SES) status and tech literacy, accepting housing and/or services at a non-profit IPA or homeless shelter. While our study results are not representative of all who experience IPA or of all populations of users in higher risk situations, it is a step in moving beyond the majority of general users in usable privacy and security research.

We conducted one-hour long, semi-structured interviews with 15 survivors of IPA who were receiving services at non-profit organizations in the U.S. Our study sought to answer the following research questions:

- What role has digital privacy and security played in the experiences that survivors of IPA have with their abusers?
- What are IPA survivors' motivations, practices, and challenges when protecting their privacy and security online and on their devices?
- What technology design implications do the digital privacy and security challenges faced by survivors of IPA suggest?

Results of the study were used to develop a framework organizing survivor technology practices and challenges into three-phases of intimate partner abuse: *physical control*, *escape*, and *life apart*. In the *physical control* phase, survivors wanted private access to devices and accounts to maintain social support and autonomy, which the abuser physically tried to limit and control. In the *escape phase*, which overlapped with both *physical control* and *life apart*, survivors faced the challenge of hiding digital escape activities (before leaving their abuser) and severing digital ties with their abuser (after leaving). In the *life apart* phase, survivors faced the challenge of preventing abusers from using digital means to find their new contact information and location. This framework provides an empirically sound method for technology creators to consider how new and existing technologies may be designed to better help survivors of IPA. The accompanying stories from survivors of IPA add nuance and render visible that they face different and complicated digital privacy and security challenges.

RELATED WORK

Here we outline prior research on the usability of privacy and security technologies, frameworks of IPA, technology use by abusers and survivors, and digital IPA interventions.

Usability of Privacy and Security Technologies

Prior research has demonstrated repeatedly that designing for privacy and security concerns is notoriously complex, many aspects of which remain highly challenging despite considerable research effort. For example, prior studies have shown that it can be difficult for users to understand the complexities of online security [26,43], Wi-Fi security [11], social media sharing mechanisms [24], and more. Thus, users sometimes adopt usage strategies with suboptimal privacy and security outcomes [26,30,43]. Taking into account these challenges, prior work has focused on improving the usability of general online privacy and security technologies [1,13,14,22,27,38]. We explore similar issues, but contribute by focusing on a specific population: survivors of IPA. Survivors are often under extraordinary stress due to their life circumstances, which may make it even more difficult for them to pay attention to the complexities of managing their digital privacy and security.

Frameworks of Intimate Partner Abuse

Survivors of IPA often find it hard and dangerous to leave their abusers [7,20,37]. Prior work from a range of fields has outlined frameworks for considering cycles and phases of IPA. According to Walker [42], survivors experience three phases of abuse: the *tension building* phase, then the *acute battering* phase of violence, and then the *honeymoon* phase during which the abuser tries to convince the survivor the abuse has ended. Walker [42], and more recent definitions of IPA from the CDC [6], include not only physical abuse but also psychological and emotional abuse, and other forms of controlling behavior.

Others have expanded Walker's work to include leaving and post-separation [3]. Much of this literature has focused on *leaving*, defined as the process of ending the abusive relationship, which can take weeks or years [37]. For example, Patton [37] described five phases of leaving: *pre-contemplation, contemplation, deciding to leave, actually leaving,* and *establishing a new violence-free life*. *Leaving* is influenced by *turning points*, or events that prompt survivors to consider escaping from their abusers [8,37], such as increased violence from abusers, life events, and changes in life-stage or beliefs [8,15,31,37,48]. For *turning points* to occur, and for survivors to maintain their lives after physically leaving their abuser, survivors need access to a variety of resources that may provide *pathways* out of abuse, including institutional support and access to information [37]. Survivors face barriers to *leaving*, such as fear of harm and dependence on abusers for necessities [37]. When survivors take steps to leave, abusers tend to significantly increase their attempts to regain control [20,46], and failed attempts to leave can result in increased severity of violence and even death [7]. Wuest and Merrit-Gray [32,47,48] studied the time after *actually leaving* an abuser physically, dividing it into three phases: *breaking free*, *not going back*, and *moving on*, during which survivors faced different challenges in establishing their

new violence-free lives, such as recovering emotionally and building new relationships.

Abusers' Uses of Technology

Abusers may use technology to track their victim's movements, or to maintain financial or psychological control. Abusers may draw on a variety of data types to track or locate survivors, including GPS, phone records, online databases, social media, hidden cameras, and spyware [20,34,40]. This can lead survivors to feel that they are "constantly under surveillance," which can increase the difficulty of leaving [45]. This tracking takes place in the context of a current or past relationship, meaning that—similar to the "insider threat" model in organizational contexts [21]—the abuser typically has intimate knowledge of and access to the survivor. This dynamic may result in increased psychological distress and violence [28]. Abusers may also use different forms of electronic communication to contact, harass, or humiliate survivors, either directly or through third parties. Abusers may try to isolate survivors by blocking access to online communication or by preventing survivors from accessing financial or other online accounts [34,45].

Survivors' Uses of Technology

The National Network to End Domestic Violence (NNEDV) has published a variety of technology-use guidelines for survivors of IPA and agencies who support them, based on extensive experience working to help this population. These guidelines cover topics including mobile phones, browsers, and social media [35].

However, survivors of IPA face considerable online privacy and security challenges. Massimi et al. [29] refer to the "complicated privacy work" survivors encounter after escaping their abusers. Survivors may rely on the same technologies abusers use to harass or find them, to help re-establish support and resources, or to document evidence of abuse [2,16,20,29]. Survivors may draw on a variety of online privacy practices, including using new devices, sharing anonymously or creating aliases, or limiting their use of online tools or sharing [2,16].

IPA-Specific Technology Interventions

Some researchers have proposed specific technology interventions to help counter the challenges and threats faced by survivors of IPA. For example, Arief et al. [5] suggest that when designing technology with the primary goal of supporting survivors, designers should take into account usability and the survivors' privacy, as well as the possibility that abusers will appropriate such technologies. Using these suggestions, they propose an app specially designed to delete evidence of the survivor's help-seeking activities, while preserving evidence of abusers' misuse of the survivors' devices. Other tools, such as *Safe Chat Silicon Valley* [49] and the NNEDV's *Tech Safety* app [35], focus on providing fast access to resources. The NNEDV's *Tech Safety* app [35] provides recommendations to survivors involving a variety of widely available privacy and security features, such as private browsing, privacy settings on social media, 2-factor authentication, and more. Another class of tools focus on allowing survivors to disguise their browsing [19]. Still other tools try to help survivors protect their physical safety. The *GuardDV* tool, for example, attempts to alert homeless IPA survivors when their abusers are nearby [25]. As an alternative approach, Clarke et al. [10] used technology-grounded processes to explore photo-sharing as a method of supporting survivors.

Combining Technology Use & Phases of IPA

We build upon prior work by developing a three-phase framework focused on the needs of the HCI community. Our framework aligns with prior work oriented to the needs of non-technology focused audiences, but does not replicate prior frameworks. For example, our first phase, *physical control,* includes the time prior to *actually leaving* from Patton [37] and prior to *breaking free* from Merrit-Gray and Wuest [32,48]. Our second phase, *escape*, begins with Patton's *deciding to leave* phase [37], and ends approximately after Merrit-Gray and Wuest's *not going back* phase [48]. Our third phase, *life apart*, begins at the point of physical separation, after *actually leaving* [37] or *breaking free* [32,48] are initiated. Our framework provides two novel contributions. First, it combines technology practices with the phases of IPA, which allows design to be considered in the context of phases. Second, although our framework was inspired by phases found in other fields, our analysis adapts them to align with the affordances of contemporary and emerging technology.

METHOD

We conducted semi-structured interviews with 15 survivors of IPA. Also as part of this research, we performed a thorough ethics review to inform our methods and reporting. We consulted the literature and over a dozen experts in domains including survivors of IPA, human subjects research, legal, ethics, security, privacy, and anonymization. Here we describe participants and recruiting, procedures, data collected, participant and researcher wellbeing, analysis, anonymization, and ethical considerations in reporting this research.

Agency Collaboration, Recruiting & Participants

Participants were survivors of IPA (14 female, 1 male), receiving services at multiple shelters run by two non-profit organizations in the U.S., which we refer to as "the agencies." The agencies served homeless adults and survivors of IPA. We worked with agency staff to co-create a study proposal and asked for advice, such as communication style, dress, location of the sessions, incentives, any follow-up that might be needed after study sessions (i.e., after care), and the gender balance of our interviewers. Once the study plan was final, agency staff recruited participants through personal contact according to criteria we specified. Specifically, participants needed to be at least 18 years of age and have an online privacy or security concern, such as experiencing an account breach. As a privacy precaution, we did not collect demographic

information from participants aside from gender. Prior to sessions, agency staff distributed a copy of our consent materials to potential participants, identifying the affiliation of the researchers, and providing them an opportunity to decline participation prior to any contact with us.

Participant & Researcher Wellbeing

We worked closely with the agencies to understand the specific sensitivities of working with their clients. To protect our participants, we met participants in-person, at agency locations where they received services and felt safe. Participants at the IPA agency were told an advocate could join them in the interview if desired; none of the participants chose to bring an advocate. We made plans with the agencies to communicate with them if anything problematic came up during interviews (such as someone revealing that they were considering self-harm in the future), and to inform participants of this after care arrangement.

Participant wellbeing shaped our study design. We sought to protect participants from undue harm from recalling painful memories, while balancing our research goals of understanding participants' experiences of online privacy and security practices and challenges. To accomplish this, we used semi-structured interviews designed to elicit stories about technology-related abuse. We intentionally omitted questions that would potentially elicit general stories related to trauma and abuse unrelated to technology. Prior work has also described the need to consider potential emotional harm to researchers [18,33]. One of the shelter directors offered to debrief the interviewer and note taker after the interviews to help process emotional responses to hearing about IPA.

Procedures & Data Collected

Sessions with survivors lasted 31-67 minutes, (μ=48). With the participants' permission, sessions were audio recorded and the resulting 14.45 hours of audio recordings were transcribed, resulting in 709 pages. (One survivor declined recording, but detailed notes were taken and analyzed with permission.) Transcripts were labeled with a pseudonym (P1, P2, etc.) and personally identifiable information within the transcripts were anonymized. Two researchers attended each session: one led the interview; the other took notes and asked occasional follow up questions. All interviews were led by the same researcher (a female); three different note-takers attended different interviews (2 females, 1 male).

We began sessions by going over the consent documents with participants, which gave permission for publication of aggregated or anonymized information. All participants gave informed consent and received a $100 gift card at the beginning of their session; the incentive amount was approved by the agencies and our organization's internal ethics review. For the remainder of the session, we used an experience-centered approach, focusing on participant experiences with technology and online privacy and security [17]. It consisted of a 5-question "ice breaker" survey about device and account use, a semi-structured interview about experiences related to digital privacy and security, and a card sort about their privacy and security practices. In this paper, we focus on results from the semi-structured interviews.

The interviews began with two neutral questions about the participant's use of technology, referencing a list of devices gathered from the ice breaker survey: (1) "Which of these devices is most important to you and why?" and (2) "Are any of these devices ever used by anyone else?" Two other questions formed the core of the interview: (3) "Can you tell me about a time when someone gained access to information about you that you did not want them to have?"; and (4) "Can you tell me about a time when someone else gained access to one of your accounts or devices? Or tried to?" To follow up on these stories, we used three questions: (a) "What happened as a result?" (b) "What did you do next?"; and (c) "How did this experience affect how you use technology?"

Analysis

We conducted inductive analysis [41], focused on 288 excerpts from the transcripts related to stories about: (1) unauthorized access to sensitive information (as defined by the participants); (2) unauthorized access to accounts or devices; and (3) abusive behavior online or with devices. Transcript content was excluded if it was a substantial repetition of a story already included, or substantially unrelated to digital privacy and security (e.g., stories about using technology for work). We developed categories, from a close reading of the transcripts, that clustered related excerpts together and conveyed key themes from the data. These categories were iteratively refined through group discussions and codified in a codebook. Each category in the codebook had a description, an example quote, and links to related subcategories. Three team members used the codebook on a sample of excerpts to ensure that the categories accurately reflected the data and that each category was adequately defined and scoped. One researcher coded the remaining data. The final codebook contained three top-level categories (*attacks*, *practices*, and *risks*) and 13 nested subcategories (e.g., under *attacks* were *controlled and monitored devices and accounts*, *hijacked account*, *online harassment*, and so on). We developed our framework's phases and applied them to the codes through group discussions.

Anonymization

Anonymizing participant information was a critical part of writing this paper. We began by consulting with three privacy experts at our organization, with extensive experience regarding data anonymization, to develop an anonymization guide. The guide focused on removing any information from participant stories and quotes that could be identifying—including to someone who was intimately familiar with them—which required a conservative approach. We did a first pass over participant information

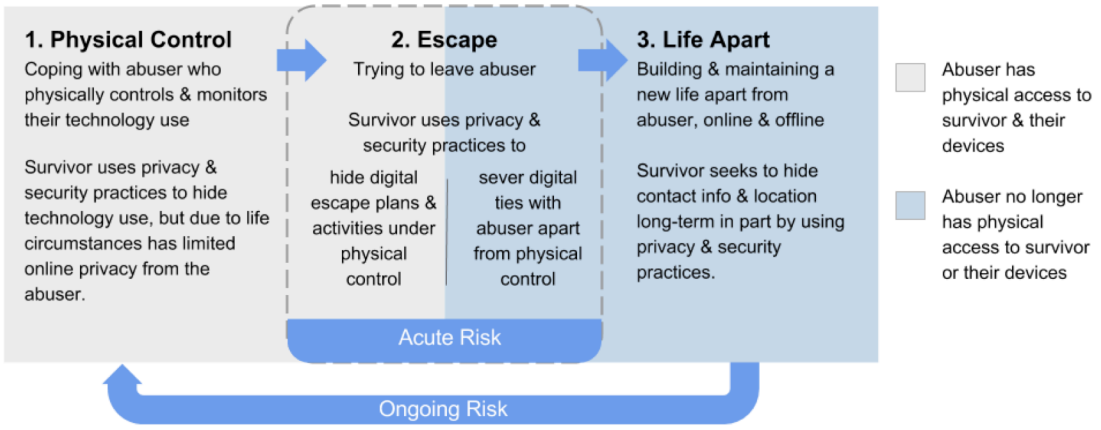

Figure 1. Three phases of IPA that affected technology use, focusing on privacy & security practices.

using the guide. We replaced specifics with more general phrases, including technologies used (e.g., "social media," "email," etc.), relationships (e.g., son or daughter would be replaced with "child"), locations, timeframes, and people's ages. We rephrased or removed unique word choices or phrases from quotations, doing so within brackets: '[]'. We inserted '[...]' where we removed words. We sometimes modified or removed filler words ("like", "you know", "kinda", "um", etc.) and unique grammar without noting where, to obscure potentially unique ways of speaking. We carefully chose participant stories that could be told without unique details. For a couple of findings shared in this paper, this was not possible (e.g., findings around deception), so we do not provide evidence to accompany those findings. After the authors' initial pass, the paper was reviewed by two of the original privacy experts and updated accordingly. Finally, a representative from one of the agencies we worked with, who was familiar with the participants' cases, reviewed the anonymization and additional modifications were made

Balancing the Risks and Benefits of Reporting Results

Before reporting this work, we considered the potential risk versus benefit of publishing participants' stories. Prior research emphasizes an ethical imperative that the results of work with survivors, who took the risk to participate, should be used to improve services and awareness among those who can improve the situation for survivors [18]. This principle can be applied to technology designers as well—those who are informed about the digital privacy and security challenges of people who experience IPA are better able to design technology that can help survivors manage their digital privacy and security.

We verified that our paper would not inform abusers before sharing it. We assessed prior literature written or peer-reviewed by people who work in the fields of advocacy for survivors of IPA. We confirmed that all our high-level findings about abuser attacks and survivor practices had been published in some form previously—if not empirical study reports, then in other widely available guidelines used by organizations supporting survivors [20,35,39,40,45].

RESULTS

Phases of IPA that Affected Technology Use

The survivors we interviewed had escaped their abusers and were in the process of finding new housing, jobs, schools for their children, and other social services. These survivors had all experienced a similar trajectory of abuse that aligned with prior work [32,37], beginning with their experiences being in a relationship with an abusive intimate partner, planning and carrying out an escape, and finally beginning a new life after leaving their abuser. We outline three phases of IPA that affected how survivors used technology: *physical control*, *escape*, and *life apart* (see Figure 1). Below, we briefly describe each phase, then describe survivors' privacy and security practices in more depth.

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." -P12

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 monitor survivors' devices and accounts and, in a few cases, install spyware on survivors' devices. Abusers exerted control over survivors' technology use and sometimes destroyed their devices. While some participants were able to use alternate devices or accounts, all described challenges maintaining autonomy and privacy using technology due to their abusive relationships. For multiple participants, the abuser's physical control of their technology use contributed to social isolation, device loss or damage, financial hardship, and psychological distress.

"I'm in isolation. [...] I've not only been isolated to my home, and to take care of my children, but isolated in that – [separated] from work and my friends. And not being able to go anywhere. So financially I'm incapacitated to do anything." -P7

Abuser Attacks Experienced		#Part.
Physical control	(a) Device/account controlled & monitored - Physical means	10
	(b) Device destroyed	4
	(c) Spyware installed	3
Cross-phase digital attacks	(d) Harassed online	8
	(e) Account hijacked - Impersonated	5
	(f) Account hijacked - Locked out	4
	(g) Account monitored - Remote or unknown means	2
Survivor Privacy & Security Practices		
(h) Limited or avoided using devices/accounts		9
(i) Limited or avoided sharing info online		9
(j) Strengthened account authentication		9
(k) Blocked contacts		8
(l) Used alternative device/account		6
(m) Deleted content or activity history		4
(n) Strengthened privacy settings		4
(o) Deactivated account		3
(p) Destroyed, discarded, or wiped device		3
(q) Monitored/restricted children's online activities		3

Table 1: Overview of survivor-reported attacks by abusers, and privacy and security practices used by survivors (N=15). From our data, we could not organize survivor practices by phase in this table, but tendencies are presented in the Results.

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 *escape*, the survivor's main goals were to leave and sever ties with their abuser. The *escape* phase overlapped with *physical control* and *life apart*. Thus it inherited the same abuser attacks and survivor practices as the other two phases (see Table 1), but added new privacy and security challenges and a higher level of risk due to survivors' life circumstances. Throughout the paper, we refer to participants who were in *escape* as also being in either *physical control* or *life apart*.

While in the *physical control* part of the *escape*, survivors focused on hiding digital escape activities, including gathering information on how to escape, setting up social support, finding new housing and jobs, and making arrangements to keep themselves and family members safe. Survivors may take considerable time to plan their escapes from abusive intimate partners [37], suggesting more robust privacy and security practices are needed to withstand an abuser's physical control over time.

In the *life apart* portion of the *escape*, survivors needed to sever digital ties with the abuser (e.g., by blocking contacts, deactivating accounts known to the abuser, limiting what they shared online, and even destroying devices). The time immediately after leaving an abuser was pivotal but tenuous [48]: the National Domestic Violence Hotline estimates that it takes an average of seven escape attempts to succeed [50]. Research shows that abusers significantly escalate their attempts to regain control over survivors during this time [20,46] and that failed escape attempts can result in increased severity of violence and even death [7]. Thus, *escape* is marked by acute risk in Figure 1 and the phases are depicted as a cycle. These prior studies, in addition to our participants' accounts, suggest that effective privacy and security practices are especially important in the time immediately after leaving an abuser.

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 the abuser finding information about them. 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), to prevent abusers from harassing them or reestablishing physical control. After severing digital ties as part of *escape*, survivors had lifelong privacy work to do, ensuring that they, their children, and other people, took great care when sharing their personal information online. Most of our participants were early in the *life apart* phase.

Next, we describe the digital privacy and security challenges and practices survivors reported (listed in Table 1[1]) during the three phases of IPA that affected technology use (outlined in Figure 1). The framework in Figure 1 was developed from post hoc analysis and we could not always tell the phase during which the attacks and practices from Table 1 occurred. Unless specified in Table 1, the items could have occurred in any of the three phases. We report tendencies in the sections below, from the stories for which the phases were clear.

[1] Note that we did not explicitly prompt participants for the specific categories in Table 1; these were all self-reported based on open ended questions about their technology use or indirect prompts. Also, survivors sometimes reported being surprised by the information abusers were able to gather about them, and they did not always know how it had happened (a problem noted in prior work [20]). Thus, the table likely under-reports less known or difficult to detect attacks (such as remote account monitoring).

Abuser Attacks Experienced

Abuser attacks differed before and after they had physical access to the survivor. During *physical control*, abusers used physical *and* digital means to control survivors' technology use. In *life apart*, abusers relied on digital attacks, such as account hijacking and online harassment.

Physical Control: Controlled, Monitored, Destroyed Devices

The most common form of physical control described by our participants was that the abuser physically controlled and monitored their device and/or account use against their will (10 participants reported, see Table 1, row a). Communications, like phone calls and text messages, were particularly of interest to participants' abusers, as P3 noted:

"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." -P3

Three participants reported that their abusers installed spyware on their devices to monitor their activity (two became aware before leaving their abusers, one after leaving; see Table 1, row c). P2 observed unusual behavior on her phone and, with help from an expert, found spyware before leaving:

"Then I took the phone to [a store] and they said this phone… somebody put something in the phone and this person can see everything you—where you call, who you talk to, all the logs." -P2

In some cases, abusers went so far as to destroy the participants' devices, to punish them and/or exert control (4 participants, see Table 1, row b). P5 told a story in which her abuser mistakenly believed she was talking to another man and punished her by destroying her phone, saying: "*he grabbed [my phone] and threw it.*" P4's abuser had destroyed several of her phones, saying *"he would just, like, stomp on it."* This isolated her from social relations: "*people have my old numbers. [...] there was no way for me to get a hold of other people.*" She had to deal with being "phoneless" for some time due to the difficulty of purchasing a new phone in her situation: *"I work hard [...] to buy myself a phone. [...] so I had to find a way [to] save without him knowing. [...] I would just hide the money."*

Cross-Phase Digital Attacks

Here we describe digital attacks employed by abusers during all phases: account hijacking and online harassment. These were the only attacks reported in *life apart*, since abusers no longer had physical access to participants and their devices.

Hijacked Accounts: Being Impersonated & Locked Out

Once abusers gained access to a survivor's account—whether through physical means before the survivor left or remotely after they left—the abuser could monitor the account and exert control over it. Two hijacking results were commonly reported by our participants. First, abusers impersonated participants in order to damage their reputations or gather information about them from their contacts (5 participants reported, see Table 1, row e). For example, P7 said her abuser monitored her email, communicated with her friends (pretending to be her), and deleted information about potential jobs.

"He read personal emails and responded to personal emails in my voice. Stuff like "Why are you harassing me?", or "Go away," or whatever. I had to do a cleanup after that. It's inconvenient. And [he] deleted job information. [...] [It was] rather personal and damaging." -P7

Her abuser's impersonated emails ruined some of P7's relationships, which led to social isolation. She said this was "*the end result, what [her abuser] wanted in the first place. And it's deeply affected my life.*" In another example, P13's abuser used one of his accounts to impersonate him in order to gather information about him from his family,

"Whenever she hacked my [social media] account she messaged everybody in my family that I didn't want her to contact, pretending to be me. [...] And she would try to get them to trust her [when] they definitely shouldn't. [...] Messaging people in my family trying to get more information about me." -P13

The second, commonly reported hijacking result was that abusers locked participants out of their accounts by changing passwords (4 participants reported, see Table 1, row f). For example, P1 explained how her abuser "*kicked [her] out*" of her social media account, because "*I think he doesn't like my friends and then that's why he did it.*"

Account hijacking limited the participants' access to technology, isolated them from their social relations, and enabled abusers to collect private information about them and harm their reputations with others.

Harassed Online & Evidence

Participants reported that abusers tried to intimidate and coerce them to stay or return by harassing them online with repeated, threatening messages (8 participants, see Table 1, row d). For example, P4's abuser posted personal details about her and threats on social media.

"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 [sibling]." -P4

Harassing messages were sometimes a double-edged sword for participants trying to escape their abusers, because these messages could also provide evidence for law enforcement. For example, P11 saved harassing messages from her abuser to obtain a restraining order.

"And so the only thing I actually kept on [the phone] was all the [...] crazy messages that he sent. When I had to get the restraining order. I kept that stuff—so the judge could see it." -P11

Survivor Privacy & Security Practices

To resist and mitigate attacks by abusers, survivors drew from the privacy and security practices in Table 1. Next, we present practices survivors tended to use in *physical control* and *life apart*, and how they addressed the needs and heightened risk of *escape* in each of these phases.

Practices During Physical Control

Due to abusers' physical control of devices, multiple survivors limited or avoided using devices and/or accounts the abuser could access (see Table 1, row h). 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."*

Without private access to the internet and communication mechanisms, participants' access to help, social relations, and jobs were severely limited. This created a high-stakes trade-off, motivating some survivors to use technology, even at the expense of significant effort and risk. For example, to hide her technology use from an abuser who constantly monitored her phone, P12 took her phone apart, hid the SD card and battery on separate parts of her body, and only checked her phone in bathroom stalls and other private locations. If her abuser got ahold of her phone, she thought he would think her phone had a dead battery.

Other practices survivors used to hide their technology use during *physical control* were to use alternate devices or delete content or activity histories (see Table 1, rows l and m). These practices became especially important once survivors decided to make escape plans, which they wanted to keep secret. P8 talked about making escape plans using an alternate email account on her computer at work.

"...at the time I was trying to look for elsewhere to live and trying to find resources and trying to apply to housing and things like that. And I didn't want [these plans] 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." -P8

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 – I once searched 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." -P2

P5 talked about emailing her friend about her abusive situation in order to get help. She thought she could hide that correspondence by deleting the relevant emails, but a misunderstanding of how delete works resulted in her abuser finding the emails.

"I have a friend that I was emailing and telling about the situation, and [my abuser] found out about it [...] it was deleted but it didn't delete out of my phone like that. He went to the archives. He went through something, and found it." -P5

This story demonstrates how the survivors' understanding of technology influenced the practices they used to hide their escape plans.

Practices During Life Apart

In *life apart*, survivors took steps to prevent abusers from finding their new locations and contact information. Immediately after physically leaving, during the *escape* phase, this often meant severing digital ties with their abusers. Over the long-term, this meant managing or limiting what they and others shared about them online.

***Escape*: Severing Digital Ties**

Some survivors deactivated their accounts as a way to hide their escape location and protect themselves from online harassment as they escaped (see Table 1, row o). For example, P3 deactivated her social media account in an effort to hide her escape 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 a high-stakes trade-off between online privacy and access to social support, both of which were critical 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.*"

More drastically, P6 destroyed her phone (see Table 1, row p). Her abuser had installed spyware on it, and she wasn't convinced that it was clean after she reset it:

"Bye-bye [...] phone [...] SIM card through the shredder. All the cards through the shredder. The phone unit, painstakingly ran over by a car a couple of times. I mean, it's in pieces." -P6

Multiple participants decided to keep their accounts, but reported strengthening account authentication (see Table 1, row j). P11 got a security notification about an unauthorized account login attempt, which prompted her to change her password and setup 2-factor authentication for her account:

"[A software product] let me know when someone's trying to hack into my account. Then I used the [2-factor authentication] method and I change 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." -P11

Long-term: Limiting Technology Use

An ongoing practice in *life apart* was to limit or avoid sharing information online (Table 1, row i). For example, before posting photos online, P5 thought very hard about whether the background of the photo might reveal the location.

"With my [child], I'll put a picture up, but I just make sure I chop the background, [...] the last picture I posted, [my child] was at [city], we were at the [city place]. You can't really tell what [place] it is. [...]. You could see cement and chairs, but you can't really see the background." -P5

However, limiting information shared online sometimes limited job opportunities, as described by two participants who had to change careers in *life apart*. For example, one participant 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." -P15

Long-term: Monitoring & Restricting Kids & Networks

An important challenge in staying hidden was that the abuser could use other people—such as the survivor's children, family, friends, colleagues, teachers, and so on—to find their contact or location information. This concern, reported by 9 participants, greatly complicated the survivors' online privacy and security work, because it required them to enlist the cooperation of other people who may not fully understand their situation.

One resulting practice for three participants was to monitor and restrict their children's online activities (Table 1, row q). For example, P9 did not allow her teenager to use social media:

"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. [He/she] could put on there [school name]. 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." –P11

P2 allowed her child to have a social media account, but she strengthened the privacy settings on her child's account and vigilantly checked them "*once or twice a month*" to ensure that her abuser—her child's father—was not able to view the survivor's profile. Similarly, multiple participants reported strengthening privacy settings (Table 1, row n).

Another resulting practice was to block contacts online, if survivors felt those contacts might threaten the survivor's safety or privacy from their abusers (Table 1, row k). For example:

"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." -P5

Protecting privacy was especially challenging for survivors who had children with their abuser, because they were sometimes legally obligated to keep communication open between the abuser and the child. Participants described using deception to hide contact information from their abusers who still had contact with their children. We omit examples as their details are too specific to anonymize.

DISCUSSION

The privacy and security practices and challenges we outline for survivors of IPA complicate simple notions of risk often used as the basis for technology design. Thus we focus discussion on commonly known issues for privacy and security technologies, for which this study of survivors broadens our understanding of user needs: usability and how much control to provide to users.

Usability of Privacy & Security Technologies

During all phases of IPA, survivors' stories demonstrated that the usability of privacy and security features is important, emphasizing findings from prior work focused on the general population [26,30,43] in a higher risk context. For example, during the *physical control* and *escape* phases survivors benefited from access to technology to maintain communication with their support network, but they also wanted to hide those communications from an abuser who had physical access to them and their devices. But survivors faced high levels of stress and risk, which may have made it harder than usual for them to pay attention to user interface details. We observed that participants made mistakes when deleting or clearing information. Designers should therefore consider both the general usability of privacy and security features, and their use during high-stress, high-risk situations.

Instructional and "help" materials that supplement technology are also valuable for survivors, who may be motivated to use privacy and security features but do not know how. For example, account hijacking was an issue for survivors across phases, and features like 2-factor authentication and security notifications of unusual account activity empowered some of our participants who knew how to use them. Further education for survivors about how to secure their accounts, such as easy-to-use security checkups, may be of value.

Usability and the availability of instructional materials may also be important for making expert-level privacy and security tools more available to survivors of IPA. For example, people regularly experiencing online harassment (such as political activists) may use expert-level tools like Tor to hide their online activity [23]. However, prior work has found that these types of tools can present usability challenges [9,36], emphasizing the importance of future work to make them more usable for highly stressed users, and to provide targeted educational materials for survivors.

Levels of Control in Privacy & Security Technologies

It is generally accepted that when designing privacy and security features, deciding how much control to provide to users involves a complicated tradeoff [12]. On one hand, increasing automation and reducing the number of options available to users can reduce complexity and human error. On the other hand, users need enough control to make appropriate contextual decisions [12]. Because of their particular life circumstances, for individuals in high-risk situations, such as survivors, the tradeoff between automation and control may be different than the general population.

In the *physical control* phase, similar to an insider threat model [21], survivors may not be able to prevent an abuser from accessing authenticated accounts or unlocked devices. Survivors may benefit from other options to hide their digital activities, especially escape plans. Some types of privacy and security options that were particularly useful to

survivors were those that enabled them to safely and privately use alternate devices (e.g., using private browsing on someone else's device), effectively control their digital traces (e.g., delete content), and maintain ambiguity and/or plausible deniability in their use of technology [4].

In the *life apart* phase, survivors would benefit from controls to deal with the complexities of staying hidden from someone whose family and social life overlaps with theirs. Learning to use controls, especially on social networking sites, was important to survivors' ability to keep their contact information and location away from their abuser. More drastically, we found that some participants deactivated accounts as part of escape plans. For survivors who feel this is the only way to sever digital ties with their abuser, technology creators could offer or continue to offer features to make the loss of a device or an account easier. For example, survivors may benefit from ways to preserve content and trusted contacts in a new account.

Online harassment was also an issue during the *escape* and *life apart* phases. Designers can help by providing or continuing to provide controls to block other users and report threatening content. However, designers should consider methods for giving survivors the option to choose to use these types of controls as appropriate in context. For example, digital channels can provide an outlet for an abuser's desire to exert control, and blocking an abuser online could lead the abuser to seek physical contact instead [20].

Technology innovators could also consider how to provide controls that help with two high stakes trade-offs survivors face during *escape* and *life apart*. First, survivors faced a tradeoff between blocking or deleting harassing messages to avoid emotional trauma, and the potential for those messages to serve as critical evidence when pressing charges against an abuser. Second, survivors may have chosen to avoid technology in an attempt to limit the information an abuser could find about them online, but this also socially isolated them at a time when they needed support and access to resources (housing, jobs, etc.). We saw that several of the practices commonly used by our participants—avoiding technology, deactivating accounts, and destroying devices—added to their social isolation. Designers should consider controls or options that can help survivors better navigate these dilemmas.

Limitations

Our sample was fairly small, and included U.S. participants primarily of lower SES, so it is not representative of all survivors of IPA. Rather, we aimed to understand a small sample of experiences in depth. Participants were not always willing to share their stories, and to protect their privacy, we are not able to share some of the specific stories they shared with us. Participants sometimes did not understand the digital attacks they experienced. Some participants spoke English as a second language and the interviewers spoke only English, which created some communication difficulties. This study had the standard limitations of self-reported data, e.g., recall and observer bias.

CONCLUSION & FUTURE WORK

We presented a qualitative study of the digital privacy and security motivations, practices, and challenges of survivors of IPA. A key contribution of this paper is a three-phase framework for organizing survivors' technology practices and challenges. This framework provides empirically sound, foundational guidance for technology creators to consider how new and existing technologies may be designed to help survivors of IPA. Generally, this framework and the stories from survivors add nuance and render visible the different and complicated kinds of digital privacy and security challenges they face given their particular life circumstances. Overall, our results suggest that usability and control of privacy and security functions should be or continue to be high priority goals of technology creators seeking to support survivors of IPA.

Future work could extend this research to other IPA survivors, including those in different SES groups, different age groups, and outside the U.S. While our study focused on adults, teens are also common victims of IPA who may have specific technology practices and needs. Careful research might also explore technological solutions to the challenges observed in our study, such as maintaining social ties without leaking personal or activity information, or balancing the need to capture digital evidence of abuse while minimizing emotional trauma. Future qualitative research could explore in-depth other technology issues that impact survivors, such as the role of technology-mediated social support in survivors' lives, or how survivors discover digital attacks by abusers.

ACKNOWLEDGEMENTS

We thank Allison Woodruff, Andreas Schou, Chao Li, Clara Sherley-Appel, Erin Simon, James Tarquin, Michael Janosko, Patrick McDonald, Thomas Roessler, and Lawrence You for their feedback and ideas regarding this paper. We thank the many people at Google and the agencies for their support and ideas as we planned and conducted this research. Most importantly, we thank our participants for their willingness to share their stories, and for their courage.

REFERENCES

1. Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, 257-272.

2. Nazanin Andalibi, Oliver L. Haimson, Munmun De Choudhury, and Andrea Forte. 2016. Understanding Social Media Disclosures of Sexual Abuse Through the Lenses of Support Seeking and Anonymity. In *Proceedings of the 2016 CHI Conference on Human*

Factors in Computing Systems, 3906–3918. https://doi.org/10.1145/2858036.2858096

3. Deborah K. Anderson and Daniel G. Saunders. 2003. Leaving An Abusive Partner An Empirical Review of Predictors, the Process of Leaving, and Psychological Well-Being. *Trauma, Violence, & Abuse* 4, 2: 163-191. https://doi.org/10.1177/1524838002250769
4. Paul M. Aoki and Allison Woodruff. 2005. Making space for stories: Ambiguity in the design of personal communication systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '05), 181-190. https://doi.org/10.1145/1054972.1054998
5. Budi Arief, Kovila PL Coopamootoo, Martin Emms, and Aad van Moorsel. 2014. Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 201-204. https://doi.org/10.1145/2665943.2665965
6. Matthew J. Breiding, Sharon G. Smith, Kathleen C. Basile, Mikel L. Walters, Jieru Chen, and Melissa T. Merrick. 2014. Prevalence and characteristics of sexual violence, stalking, and intimate partner violence victimization-National Intimate Partner and Sexual Violence Survey, United States, 2011. *Morbidity and Mortality Weekly Report* 63, 4: 1-18. https://doi.org/10.2105/AJPH.2015.302634
7. Jacquelyn C. Campbell, Daniel Webster, Jane Koziol-McLain, Carolyn Block, Doris Campbell, Mary Ann Curry, Faye Gary, Nancy Glass, Judith McFarlane, Carolyn Sachs, and others. 2003. Risk factors for femicide in abusive relationships: Results from a multisite case control study. *American Journal of Public Health* 93, 7: 1089-1097. https://doi.org/10.2105/AJPH.93.7.1089
8. Judy C. Chang, Diane Dado, Lynn Hawker, Patricia A. Cluss, Raquel Buranosky, Leslie Slagel, Melissa McNeil, and Sarah Hudson Scholle. 2010. Understanding turning points in intimate partner violence: Factors and circumstances leading women victims toward change. *Journal of Women's Health* 19, 2: 251-259. https://doi.org/10.1089/jwh.2009.1568
9. Jeremy Clark, P. C. van Oorschot, and Carlisle Adams. 2007. Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (SOUPS '07), 41-51. https://doi.org/10.1145/1280680.1280687
10. Rachel Clarke, Peter Wright, Madeline Balaam, and John McCarthy. 2013. Digital Portraits: Photo-sharing After Domestic Violence. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13), 2517-2526. https://doi.org/10.1145/2470654.2481348
11. Sunny Consolvo, Jaeyeon Jung, Ben Greenstein, Pauline Powledge, Gabriel Maganis, and Daniel Avrahami. 2010. The Wi-Fi privacy ticker: Improving awareness & control of personal information exposure on Wi-Fi. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (UBICOMP '10)*, 321-330. https://doi.org/10.1145/1864349.1864398
12. Lorrie Faith Cranor. 2008. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08)*. 1-15.
13. Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law* 10, 2: 273-307.
14. Lorrie Faith Cranor and Simson Garfinkel. 2005. *Security and usability: Designing secure systems that people can use*. O'Reilly Media, Inc.
15. Sally A. Matar Curnow. 1997. The open window phase: Helpseeking and reality behaviors by battered women. *Applied Nursing Research* 10, 3: 128-135. https://doi.org/10.1016/S0897-1897(97)80215-7
16. Jill P. Dimond, Casey Fiesler, and Amy S. Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5: 413-421. https://doi.org/10.1016/j.intcom.2011.04.006
17. Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the Experience-Centeredness of Privacy and Security Technologies. In *Proceedings of the 2014 Workshop on New Security Paradigms Workshop* (NSPW '14), 83-94. https://doi.org/10.1145/2683467.2683475
18. Mary Ellsberg and Lori Heise. 2002. Bearing witness: Ethics in domestic violence research. *The Lancet* 359, 9317: 1599-1604. https://doi.org/10.1016/S0140-6736(02)08521-5
19. Martin Emms, Budi Arief, and Aad van Moorsel. 2014. Electronic footprints in the sand: Technologies for assisting domestic violence survivors. In *Privacy Technologies and Policy*, 203-214.
20. Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth, and Sarah Tucker. 2010. The new age of stalking: Technological implications for stalking. *Juvenile and family court journal* 61, 4: 39-55. https://doi.org/10.1111/j.1755-6988.2010.01051.x

21. Jeffrey Hunker and Christian W. Probst. 2011. Insiders and Insider Threats. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications* 2, 1: 4-27.
22. Giovanni Iachello and Jason Hong. 2007. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction* 1, 1: 1-137. https://doi.org/10.1561/1100000004
23. Eric Jardine. 2015. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Global Commission on Internet Governance Paper Series, No. 21. https://ssrn.com/abstract=2667711
24. Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and privacy: It's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*, 9. https://doi.org/10.1145/2335356.2335369
25. Zayira Jordán Conde, William Eric Marsh, Andrew W. Luse, and Li-Shan Eva Tao. 2008. GuardDV: A proximity detection device for homeless survivors of domestic violence. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, 3855-3860. https://doi.org/10.1145/1358628.1358943
26. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS '15)*, 39-52.
27. Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*, 2595-2604. https://doi.org/10.1145/1978942.1979321
28. T. K. Logan and Robert Walker. 2009. Partner stalking: Psychological dominance or "business as usual?" *Trauma Violence Abuse* 10, 3. https://doi.org/10.1177/1524838009334461
29. Michael Massimi, Jill P. Dimond, and Christopher A. Le Dantec. 2012. Finding a new normal: The role of technology in life disruptions. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW '12)*, 719-728. https://doi.org/10.1145/2145204.2145314
30. Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, and others. 2010. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, 645-654. https://doi.org/10.1145/1753326.1753421
31. Judith McFarlane, Ann Malecha, Julia Gist, Kathy Watson, Elizabeth Batten, Iva Hall, and Sheila Smith. 2004. Increasing the safety-promoting behaviors of abused women. *AJN The American Journal of Nursing* 104, 3: 40-50.
32. M. Merritt-Gray and J. Wuest. 1995. Counteracting abuse and breaking free: The process of leaving revealed through women's voices. *Health Care for Women International* 16, 5: 399-412. https://doi.org/10.1080/07399339509516194
33. Wendy Moncur. 2013. The Emotional Wellbeing of Researchers: Considerations for Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13), 1883-1890. https://doi.org/10.1145/2470654.2466248
34. NNEDV. Power and Control Wheel. Retrieved September 17, 2016 from http://nnedv.org/resources/transitional-housing/139-financial-empowerment-economic-justice-resources/3898-power-and-control-wheel.html
35. NNEDV. Tech Safety App. Retrieved September 17, 2016 from http://techsafetyapp.org/
36. Greg Norcie, Kelly Caine, and L. Jean Camp. 2012. Eliminating stop-points in the installation and use of anonymity systems: a usability evaluation of the tor browser bundle. In *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS)*.
37. Shirley Patton. 2003. *Pathways: How women leave violent men*. Government of Tasmania. http://nla.gov.au/anbd.bib-an25304195
38. Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the "weakest link"—a human/computer interaction approach to usable and effective security. *BT Technology Journal* 19, 3: 122-131. https://doi.org/10.1023/A:1011902718709
39. Cindy Southworth, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2005. A high-tech twist on abuse: Technology, intimate partner stalking, and advocacy. *Violence Against Women Online Resources*. Retrieved January 3, 2017 from http://www.vawnet.org
40. Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. Intimate partner violence, technology, and stalking. *Violence Against Women* 13, 8: 842-856. https://doi.org/10.1177/1077801207302045
41. David R. Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation* 27, 2: 237-246.

42. Lenore E. Walker. 1977. Battered women and learned helplessness. *Victimology* 2, 3-4: 525-534. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=46167

43. Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. https://doi.org/10.1145/1837110.1837125

44. WHO, Department of Reproductive Health and Research, and London School of Hygiene and Tropical Medicine, South African Medical Research Council. 2013. *Global and regional estimates of violence against women: Prevalence and health effects of intimate partner violence and non-partner sexual violence*. World Health Organization. Retrieved from http://www.who.int/iris/handle/10665/85239

45. Delanie Woodlock. 2016. The abuse of technology in domestic violence and stalking. *Violence Against Women*. https://doi.org/10.1177/1077801216646277

46. World Health Organization. 2002. World Report on Violence and Health. Edited by Etienne G. Krug, Linda L. Dahlberg, et al. http://www.who.int/violence_injury_prevention/violence/world_report/

47. J. Wuest and M. Merritt-Gray. 2001. Beyond survival: Reclaiming self after leaving an abusive male partner. *The Canadian Journal of Nursing Research* 32, 4: 79-94.

48. Judith Wuest and Marilyn Merritt-Gray. 1999. Not Going Back: Sustaining the Separation in the Process of Leaving Abusive Relationships. *Violence Against Women* 5, 2: 110-133.

49. Safe Chat Silicon Valley. Retrieved September 17, 2016 from http://safechatsv.com/about-us/

50. The National Domestic Violence Hotline: 50 Obstacles to Leaving: 1-10. Retrieved September 17, 2016 from http://www.thehotline.org/2013/06/50-obstacles-to-leaving-1-10/