"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology

Diana Freed[†] **Jackeline Palmer**[‡] **Diana Minchala**[Ψ] **Karen Levy**[Φ] **Thomas Ristenpart**[†] **Nicola Dell**[†]

[†] Cornell Tech
{dlf92,ristenpart,nixdell}
@cornell.edu

[‡] Hunter College
jackeline.palmer
@macaulay.cuny.edu

[Ψ] City College of New York
minchala.diana652
@gmail.com

[Φ] Cornell University
karen.levy
@cornell.edu

ABSTRACT

This paper describes a qualitative study with 89 participants that details how abusers in intimate partner violence (IPV) contexts exploit technologies to intimidate, threaten, monitor, impersonate, harass, or otherwise harm their victims. We show that, at their core, many of the attacks in IPV contexts are technologically unsophisticated from the perspective of a security practitioner or researcher. For example, they are often carried out by a *UI-bound adversary*—an adversarial but authenticated user that interacts with a victim's device or account via standard user interfaces—or by downloading and installing a ready-made application that enables spying on a victim. Nevertheless, we show how the sociotechnical and relational factors that characterize IPV make such attacks both extremely damaging to victims and challenging to counteract, in part because they undermine the predominant threat models under which systems have been designed. We discuss the nature of these new IPV threat models and outline opportunities for HCI research and design to mitigate these attacks.

ACM Classification Keywords

H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

Author Keywords

IPV; intimate partner violence; domestic violence; violence against women; domestic abuse; privacy; safety; security.

INTRODUCTION

As digital technologies become more deeply woven into all aspects of our lives, an increasing number of threats result from technology-related abuse, including online harassment [22, 47, 51], cyberstalking [17, 18, 20], doxxing [5, 15], and cyberbullying [2, 14]. Our paper examines technology-related abuse in the context of intimate partner violence (IPV), a serious societal problem that affects one in three women and one in six men in the course of their lives [40]. The HCI community has demonstrated a growing interest in understanding technology's role in IPV, with Dimond et al. [13] discussing how victims are harassed via mobile phones, Matthews et al. [28] detailing survivor coping strategies, and Freed at al. [21] analyzing the ecosystem of services surrounding IPV.

Our paper builds on this literature with the most in-depth analysis to date of how abusers in IPV exploit technologies to perpetuate their abuse. In collaboration with the New York City Mayor's Office to Combat Domestic Violence, we conducted 11 focus groups with 39 survivors of IPV and interviews with 50 professionals that, among them, have served hundreds of IPV survivors. We provide the first analysis of how prevalent computer security and privacy mechanisms fail victims of IPV, use these insights to characterize new threat models that better fit IPV contexts, and propose new tools that address some of the technology challenges faced by victims of IPV.

At a high level, our analysis shows that conventional threat models, and the countermeasures based on them, do not anticipate attackers who possess such intimate knowledge of, and access to, victims. Abusers frequently take advantage of the fact that they may be the legal owners of their victims' devices or online accounts. Abusers also compromise victims' accounts by guessing their passwords or forcing them to disclose them, which in turn enables digital tracking, installation of spyware, denial of access to devices or the Internet, and more. We also detail how abusers harass and intimidate their victims via hurtful messaging or posts, or publicly reveal sensitive and intimate information to humiliate and harm them. Although many of these attacks are not technically sophisticated from the perspective of security researchers, they represent the way that a large number of vulnerable people experience (in)security every day, and their technical simplicity belies the challenges that must be overcome to prevent them.

We therefore contribute new frameworks to guide future HCI research and design towards combating technology-related IPV. Specifically, we detail a new threat model characterized by a *UI-bound adversary*—an authenticated but adversarial user of a victim's device or account who carries out attacks by interacting with the standard user interface, rather than through the installation of malicious or sophisticated software tools. We describe how there is scope for redesigning UIs and underlying systems in ways that better combat this threat model. Systems could be designed that attempt to distinguish between the abuser's and victim's use of the system based on behavioral or contextual cues, or covert authentication

CHI 2018, April 21–26, 2018, Montreal, QC, Canada

 ISBN 978-1-4503-5620-6/18/04…$15.00

DOI: https://doi.org/10.1145/3173574.3174241

mechanisms could be designed to help victims hide content on their devices from UI-bound adversaries.

More generally, we argue for the need for IPV safety reviews in HCI design. These would aim to ensure that designers create systems that provide high levels of usability for legitimate users, while degrading usability for abusers (e.g., by hiding or removing functionality that would be primarily of interest to abusers). Finally, we address the seemingly prevalent use of ready-made apps that enable abusers to remotely spy on victims. In addition to apps that are explicitly advertised as spyware, our data shows that abusers frequently exploit *dual-use* applications—tools whose main purpose is legitimate but that can be easily repurposed to function as spyware (e.g., parental control and "Find My Friends" apps). We demonstrate a need for new tools that detect and mitigate both spyware and dual-use software within the complexities of IPV contexts.

In summary, our paper makes three contributions to the HCI community. First, we develop a nuanced understanding of the numerous ways in which abusers exploit digital technologies to intimidate, threaten, monitor, impersonate, harass, or otherwise harm their victims. Second, we distill new threat models that characterize abuser interactions with technology and explain the deficiencies of current security and privacy mechanisms for these contexts. Finally, we discuss concrete ideas for designing new tools that constructively address some of the technology-related challenges faced by victims of IPV.

BACKGROUND AND RELATED WORK

IPV is a prevalent global problem that affects millions of people worldwide [11, 44] with recent reports suggesting that one in three women and one in six men experience IPV at some point in their lives [40]. A significant amount of research outside of HCI has examined the nature of IPV [12, 34]. For example, researchers have considered factors that enable IPV survivors to recognize their situations as abusive [8, 48] and why it is so difficult for victims to leave abusers [7, 20, 32]. Researchers have studied abuser tactics and created materials, such as the Power and Control Wheel [33, 53] and the Composite Abuse Scale [10, 19], to understand and explain abuser behavior, with a particular focus on physical and sexual violence. However, none of these existing materials consider how abusers use technology to perpetuate their abuse.

Outside the IPV context, an increasing amount of research analyzes how technology can be used to harm and abuse others. For example, Eterovic-Soric et al. [18] provide a review of technologies used by stalkers. Other well-studied types of technology-enabled abuse include online harassment [22, 47, 51], doxxing [5, 15], cyberbullying [2, 14], and cyberstalking [17, 20, 38]. Although these non-intimate forms of abuse share some characteristics with IPV (e.g., abusers may release sensitive information about the victim online), the key difference between these contexts and our focus is that, in IPV, the abuser and victim share an intimate relationship in the physical world as well. This changes the nature of the attacks and enables abusers to use their intimate knowledge of victims to inflict additional harm.

Advocates who work with IPV survivors have long recognized the threat of technology and the need to develop legal and safety planning strategies for dealing with technology-enabled abuse [41–43]. Subsequently, academics have initiated more formal study of technology in IPV, with most studies using qualitative methods. In 2011, Dimond et al. [13] interviewed 10 female IPV survivors living in a shelter and documented how technology affected their experiences, pointing out the need for additional empirical work to closely examine technology-enabled IPV, particularly on social media platforms. Woodlock [52] used online surveys to study technology-facilitated IPV in Australia, providing quantitative statistics on some of the ways in which abusers exploit technology and calling for technology-facilitated stalking to be treated as a serious offense by policy and legal professionals.

Matthews et al. [28] interviewed 15 IPV survivors, focusing primarily on understanding survivor strategies for coping with technology-related abuse. Their paper calls for future work to engage with a larger, more socioeconomically diverse sample. Most recently, Freed et al. [21] conducted a multi-stakeholder analysis of technology's role in IPV, discussing survivors' knowledge of technology, how advocates identify technology-related abuse, and legal challenges that make technology difficult to deal with in IPV. A subset of the data used in this paper was used in [21], but here we have a complementary focus on abuser strategies and, consequently, our analysis of the dataset is much different (see the next section).

Our paper extends these prior works in a number of important ways, and specifically speaks to prior works' calls for more in-depth analysis focused on abuser attack strategies. Our study engages with 89 participants: 39 survivors that have personally experienced IPV and 50 professionals that, among them, have provided services to hundreds of IPV victims. Our participants are drawn from all five boroughs in New York City and possess a wide range of cultural, racial, and socioeconomic backgrounds. Our analysis of the resulting dataset both validates many of the issues raised in previous papers [13,21,28,52], and paints a far richer picture of technology abuse in IPV. For example, we highlight in the following sections fully 27 different types of attacks victims are experiencing. We are also the first to detail threat models that capture important classes of attacks in this setting, characterize how current security and privacy mechanisms fail victims of IPV, and provide constructive, actionable ideas for tools to address some of the challenges faced by IPV victims.

METHODOLOGY

Our qualitative study took place in New York City (NYC) in collaboration with the Mayor's Office to Combat Domestic Violence (OCDV)[1] and their five Family Justice Centers (FJCs)[2]. The FJCs provide a crucial point of contact between survivors of IPV and a wide range of public services, including housing, legal, financial, social, and other supportive services. Through the FJCs, the OCDV is also able to provide survivors of IPV with access to non-profit organizations, key city agencies, law

[1] www.nyc.gov/domesticviolence

[2] http://www1.nyc.gov/site/ocdv/programs/family-justice-centers.page

enforcement, and the District Attorney's offices. Our research engaged directly with both survivors of IPV and with a wide range of professionals who provide services to survivors of IPV, including social workers, psychiatrists, case managers, attorneys, law enforcement, and others, as described below. Before beginning our research we received approval for all study procedures from our university's IRB and from the OCDV.

Focus Groups with Survivors of IPV

We conducted 11 focus groups with a total of 39 survivors of IPV who were clients at the FJCs. To recruit survivors, we placed fliers (in English and Spanish) in the FJC reception area. Survivors who were interested in participating contacted the Deputy Director who helped us to schedule focus groups. The focus groups took place on site at the FJCs and, at the suggestion of the OCDV, we provided refreshments and compensated each participant with $10 for their time. We were advised by the OCDV to meet with survivors in groups because they would likely be more comfortable in a group setting, be more willing to discuss their experiences, and benefit from hearing fellow survivors share similar experiences.

Each focus group lasted 60–90 minutes and ranged in size from two to ten participants. The focus group discussions were structured around a set of high level topics. We asked participants about the technologies that they owned and used, the ways in which technology had come up in their abusive relationship, their strategies for defending themselves, and their ideas and needs for what would help them to better cope with technology-enabled abuse. Since many of the survivors spoke Spanish, we held focus groups in both English (8 groups) and Spanish (3 groups). For the Spanish groups, the first author asked questions in English, which were translated into Spanish by another team member (the second and third authors are fluent Spanish speakers). Participants responded in Spanish and their answers were translated into English. All focus groups were audio-recorded and transcribed prior to analysis.

We were careful to protect participants' privacy and safety. We did not ask participants to sign a consent form since we did not want to record any identifying information (e.g., their names). Although we provided printouts with information about the study we explained that, if participants chose to take the printout home, someone might learn they had attended the focus group at the FJC. We also told participants that an experienced case worker was available at all times to speak with them to help them process any upsetting experiences.

Semi-Structured Interviews with IPV Professionals

We conducted semi-structured interviews with 50 professionals who provide services to survivors of IPV. To recruit professionals, we asked the FJC Deputy Directors to make their employees aware of the opportunity to participate in the study. Interested professionals contacted the Deputy Director who helped us schedule one-on-one interviews. The interviews were in English and lasted roughly 30 minutes. We asked about participants' demographic characteristics, professional and educational background, experience working with survivors, types of technology abuse encountered, and advice given to survivors in these situations. All interviews were done by the first author with another team member present to take notes. All but one of the interviews were audio-recorded and transcribed prior to analysis. One participant requested that we not audio-record the interview, and so we captured it through detailed handwritten notes. We did not compensate professional participants at the suggestion of the OCDV.

39 survivors		
Gender	Female: 39 Male: 0	
Age (years)	Min: 18 Max: 65 Average: 42	
Regions of Origin	Africa, Asia, Caribbean, Central America, Europe, North America, South America	
Research Sites		English / Spanish
	FJC A:	6 / 0
	FJC B:	2 / 6
	FJC C:	4 / 10
	FJC D:	5 / 4
	FJC E:	2 / 0
Education	Did not complete high school:	5
	Completed high school:	14
	Attended college, did not graduate:	6
	Completed college:	9
	Unreported:	5
Living Status	With partner:	1
	Without partner:	28
	Shelter:	9
	Unreported:	1
Children	Yes: 33 No: 5 Unreported: 1	
50 professionals		
Gender	Female: 45 Male: 5	
Age (years)	Min: 22 Max: 56 Average: 33	
Research sites	FJC A: 7 FJC B: 12 FJC C: 11 FJC D: 10 FJC E: 10	
Professional roles	Case manager/case worker:	18
	Social worker	14
	Attorneys/paralegals	11
	Police officers	7

Table 1. Summary of participants' demographic characteristics.

Participant Characteristics

We recruited a total of 89 participants (39 survivors and 50 professionals) from five FJCs. As shown in Table 1, our survivor participants were all female, ranged in age from 18 to 65 years (average = 42 years), came from a wide range of countries, and had diverse educational backgrounds. All except one reported that they no longer lived with their abuser. Our 50 professional participants consisted of 45 females and five males, ranging in age from 22 to 56 years (average = 33 years). Our participants worked in a wide range of roles, including social workers, case workers, attorneys, and police.

Data Analysis

We collected over 39 hours of audio recordings that resulted in approximately 1,000 pages of transcripts. While a subset of this data was used in prior work by Freed et al. [21], we focus here on abuser strategies as opposed to the broader

ecosystem of stakelholders and, consequently, we conducted a completely fresh thematic analysis [9] of the data. We began with a comprehensive reading of the transcripts during which we identified codes. Our initial pass through the data resulted in roughly 80 codes (e.g., *remote surveillance*, *child tracked*, *location tracking*, and *password disclosure*). We then iteratively refined and discussed the codes to ensure that they were representative of the data. The resulting codes were formalized in a codebook that was used to perform a detailed analysis of all the transcripts. Related codes were then clustered into high-level themes that represent our prominent findings.

Ethics

One goal of our research is to detail the diverse ways in which technology is being used by abusers to harm victims of IPV. In publishing this information, we are keenly aware that abusers might learn new ways to abuse from our data. However, our research shows that *technology-related abuse is already extremely prevalent in IPV*. Therefore, we believe it is critically important to bring the details of these attacks to the attention of the computer security and privacy community. Indeed, many participants said they wanted their stories to be heard in the hope that they would motivate researchers to work on the challenges presented by IPV. In reporting our data, we have taken steps to protect the anonymity of participants. The stories and attacks that we describe came up frequently and are *not* intended to illustrate any individual's unique situation. In some cases, we have altered the wording of quotes slightly to remove potentially identifying phrasing.

Limitations

We acknowledge that our study has several methodological and sampling limitations. For example, although IPV affects people of all genders, all of our survivor participants were women. In addition, the majority of participants had left their abusive relationship. Finally, with a few exceptions, most participants' abusive relationships were heterosexual, and LGBTQIA+ relationships may present additional challenges.

FINDINGS

Our analysis reveals the numerous ways in which abusers in IPV exploit technology (see Table 2). We categorize attacks into four broad categories. Abusers take advantage of **ownership of devices or online accounts** used by victims, or use knowledge gleaned during their intimate relationship to surreptitiously **compromise devices or accounts**. This allows digital tracking, installing spyware, denying the victim access to devices or the Internet, and more. In addition to these access-based attacks, we explore attacks that do *not* require access: harassment, threats, and intimidation via **hurtful messaging or posts**, and **exposure-based harms** that arise when abusers publicly reveal sensitive information about the victim.

Ownership of Devices and Accounts

One of the defining characteristics of IPV that differentiates it from other types of abuse or harassment is that the abuser and victim have (or have had) an intimate relationship in the physical world. Many of our survivor participants were married to their abusers and shared common social networks, children, and physical space. The longevity and complexity of these intimate relationships often results in a set of attacks that stem from the fact that the abuser is in fact the legal owner of the survivor's devices or accounts. We now discuss these attacks.

How abusers gain ownership-based access

Many participants (n=20) described how abusers bought and paid for the physical devices that the victims use:

> *"I didn't have a phone so my husband bought me a phone . . . he put it in his name and he gave it to me, and until this day . . . the number shows his name, and he has access to the phone. I called the phone company, but they won't let me change it, because it's in his name."* (P26, survivor)

Being the owner of the device also gave the abuser the power to physically take the device away from the victim as a form of control, with one participant sharing that *"as soon as you argue, it's "Give me my phone"."* In addition, abusers often destroyed their victims' devices, which both intimidated the victim and cut off their ability to use the device for communication. At least eight victims reported this, with one telling us *"whenever he suspected that I was cheating, he would smash the phone."* We also heard how abusers would physically take the device away from victims and/or destroy it to prevent them from being able to call the police and report the abuse:

> *"There are a lot of times that I feel like I can't call the cops because he's going to take the phone. Or you know, I'm just not going to be able to get to the phone in time. [One] day, he did take the phones, he took the house phone, the cellphone, the iPad."* (P39, survivor)

In addition to owning or controlling the physical devices, many participants (n=27) reported that abusers frequently controlled victims' *digital* accounts. Often, this control stemmed from the victim and abuser sharing a mobile "family plan." In these situations, the abuser often receives phone bills that provide them with detailed information about the survivor's call history, text messages, and voicemails. Survivors described how they were unaware, when they received a phone or set up a family plan, of the level of access that it would give the abuser:

> *"[The abuser] was the one who got a phone from [phone company], it was his account . . . he can see everybody I talk to. He probably had access to my voice mail. I just learned that somebody can access your voice mail. I don't know what he was doing."* (P31, survivor).

We also heard of at least ten cases where abusers gave devices to *children* that they shared with the survivor, which provides additional control and access to the survivor even after they have managed to leave the relationship:

> *". . . especially if they're separated and having custody issues, the abuser will give a cellphone to one of the kids. And the kid is so excited, they get a cellphone, but [the abuser] uses it as a way of getting in and figuring out what's going on in the home."* (P20, social worker)

In such situations, since the abuser is legally entitled to contact the child, the victim may not be allowed to remove the device.

Ownership-based access	Have access by…	Being "owner" of device or account Shared accounts / family plans Buying children devices
	Use access to…	Physically prevent use of device/account (e.g., to call police) Digitally control access (e.g., turn off Internet) Physically destroy device Track victim's location, monitor usage, etc. via "owned" accounts or family plan
Account/device compromise	Compromise by…	Forcing victim to reveal passwords (e.g., via physical threats) Inspecting device without victim's knowledge Remotely "hacking" security questions or passwords
	Use access to…	Install spyware on device(s) Monitor victim through dual-use "legitimate" app Track victim by monitoring location Monitor victim's application use (text, email, FB, etc.) Steal victim's info (e.g., contact numbers, bank accounts) Delete victim's data (e.g., evidence, removes friends, deletes messages) Lock victim out by changing password, setting up 2-factor authentication, etc. Impersonate victim using their accounts to cause them harm
Harmful messages or posts	Call/text/message victim from identifiable account(s) Call/text/message victim from anonymized account (e.g., spoofed phone number, fake Facebook profile) Post content to humiliate/harm victim (e.g., threats of violence on social media) Harass victim's friends and family Facilitate harassment by third parties (e.g., abuser's new intimate partner)	
Exposure of private information	Threaten to expose information to blackmail victim (e.g., into not reporting the abuse) Posting private information ("doxxing") about victim (e.g., HIV status, sexual orientation) Revenge porn, non-consensual pornography, posting intimate images Create fake profiles/advertisements advertising sexual services of victim	

Table 2. Summary of attacks by abusers grouped into four categories.

How abusers exploit ownership-based access

As the owner of the survivor's or children's devices and accounts, abusers are able to exploit the data back-up services offered by providers. Many of these services can be configured to automatically transmit *all* of the data associated with a device or account to the cloud, including texts, call logs, pictures, and location. Our data shows that abusers exploit these back-up services to keep track of their victim's activities, with or without the victim's knowledge. A police officer shared:

> *"When it comes to iPhones, if they have an iCloud, I say, "You've got to get your own account because that person is always going to have access to your phone through the iCloud". Through there, you could get Where's My Phone and find the location."* (P26, police officer)

We heard numerous (n=47) accounts of how abusers used location-based services to track victim devices, including anti-theft services (e.g., 'Find My Phone'), parental tracking, and other safety-based services (e.g., 'Find My Friends'). Many survivors were unaware that their location could be tracked using these services and asked us to teach them how to turn off location services on their phone. Professionals also described how survivors' lack of awareness regarding location tracking may result in potentially dangerous physical stalking:

> *"…an abusive partner kicked in our front door and wound up in the lobby of our [building] by tracking her phone … it was some secondary application that [the abuser] had put on it and knew exactly where she was. He literally kicked our front door open. We called the police … it was scary."* (P35, case manager)

In response to ownership-based attacks, IPV professionals told us that one of the first pieces of advice they give to survivors is to purchase a new device that is not owned by the abuser. However, in many cases, the abuser is the sole financial provider for the family and the survivor is unable to afford the cost of a new device or mobile plan. A case worker described:

> *"Let's say you pay for my phone. If I leave you, you're going to cut my phone off … I need that phone because my grandmother has to contact me. My grandmother is sick and this is the only number she has. I don't have any money to buy another phone. So now, you're controlling my phone. If I don't do as you say, you're going to cut my phone off. I've seen that happen."* (P22, case worker)

Account or Device Compromise

In addition to attacks that are facilitated by abusers' ownership or financial control of accounts and devices, our analysis reveals a diverse set of scenarios in which abusers are able to compromise victims' devices or accounts against their will and/or without their knowledge. Such compromises predominantly occurred via two routes: compelled password disclosure and remote compromise of accounts by guessing of victim passwords or the answers to password reset security questions. Once a compromise occurred, attackers tended to extract sensitive or delete important information and, in the case of devices, install applications that can be used for spying on victims.

How abusers compromise devices and accounts

Abusers used a range of strategies to coerce or force victims to hand over their passwords. Many participants (n=28) described how victims had been convinced to share their pass-

words when the relationship was still *"good"* as a way of assuring their partner that they could be trusted. Once the relationship turned *"bad,"*, abusers often used their control over the victim to force them to disclose their password, making threats such as *"give me your password or get out of my house."* Alternatively, abusers might physically harm the victim if they did not hand over their passwords. A case manager said:

> *"A lot of cases have begun with 'he or she asked for my password and I wouldn't give it to them, but eventually I had to.' It's a lot of that control part of domestic violence, where [the victim] feels like they have to do it and so they do. And that's how a lot of it begins with [the abuser] having access."* (P15, case manager)

Cohabitation also made it easy for an abuser to go through a victim's device when they were not looking, with at least 16 participants reporting this attack. This either required knowledge of the victim's PIN or password, or the device to be unlocked. In some cases such device access in turn enabled access to automatically saved account passwords:

> *"[The abuser] stole her computer and was able to access all this information . . . her school applications, her bank accounts, all sorts of things, and gain access and control of these things. That . . . had a totally traumatizing effect."* (P31, case manager)

Many participants (n=26) also reported that abusers were able to *"hack"* into victim accounts. We found that the typical vectors of remote account compromises are technically mundane. Frequently, abusers are able to use their knowledge of the victim's personal details to infer passwords or correctly answer their security questions and reset their password:

> *"They'll hack into their phones and they'll hack into their accounts. Especially with intimate partner victimization . . . oftentimes these people share and know what is very personal information . . . because that was not something that they necessarily kept private when the relationship was a trusting, loving, good one."* (P3, case manager)

Often the ability to compromise accounts persisted across victim attempts to prevent abuser access. At least seven survivors said that it did not matter what they did or what new accounts they opened, the abuser always managed to gain access.

How abusers exploit access to devices and accounts

Regardless of how they gained access to victim devices or accounts, and as alluded to in the quotations above, abusers used their access to monitor, control, impersonate, or otherwise hurt their victims. One prevalent strategy was for the abuser to simply take over the account and make changes that prevented the victim from being able to access their own accounts (e.g., changing the password). Abusers were also able to successfully set up two-factor authentication for the account that would prevent the victim from being able to reclaim it:

> *"The [abuser] hacked their Facebook, hacked their email, hacked the phone. So you know how Facebook will send you a text message, like a code to let you in. So trying to somehow report it and give her access so she can change everything again was hard, because the phone number that was listed was a number that he had in his possession. So it was impossible."* (P30, case manager)

Participants also described how abusers would *"go through"* their device to monitor who they had been in contact with. They also read messages, deleted content, and removed contacts or friends that they did not approve of. Several (n=9) survivors also described how their abuser had discovered and deleted evidence of the abuse that the survivor had collected:

> *"I had a journal where I wrote down about things that were happening, altercations, and I had evidence of what was going on. He told me that he needed to update the device. He took the phone, forced the password out of me . . . and he deleted [my journal]."* (P3, survivor)

Another tactic was for the abuser to save all of the victim's contacts' information so that, if the victim decided to change their name, accounts, or phone number, the abuser could contact their friends and family and track them down. At least 28 participants said that abusers stole personal content stored on victims' devices, including intimate images, which the abuser would then use to blackmail the victim or destroy their reputation. Finally, abusers used their access to victims' accounts to impersonate them, often with the goal of isolating victims from their social support networks. For example, one participant described how, when she was looking for a job, her abuser would contact all her potential employers pretending to be her and sabotage any meetings that she had set up. Others described how their abusers would send messages to their Facebook friends that appeared to be coming from the victim, and that were explicitly intended to damage their friendships.

Spyware and dual-use applications

Our data suggests that abusers often install software that enables spying on the victim. Although we heard of three cases where the presence of such spyware was confirmed (for example, by taking the device to be inspected at a store), it was much more common (n=15) for participants to merely *suspect* that the abuser had *"put something"* on their device based on information that the abuser seemed to know, such as specific details of victims' calls, texts, email, social media, and more:

> *"Spyware, spoofing . . . [the abuser] will be able to get into text conversations they had with their family or friends, to know everything that's written in their emails. I've had survivors where it was very clear that [the abuser] had been hacking their computers. They had complete control."* (P38, social worker)

Despite suspecting the presence of spyware on survivors' devices, neither professionals nor survivors were able to name any specific spyware tools or applications that they had encountered. In addition, none of our participants had used antivirus software or other tools to discover or remove suspicious applications from their devices.

Our data also revealed how abusers often leverage what we term *dual-use* applications to spy on victims. Unlike software that is clearly designed and marketed to be spyware, dual-use applications are designed for legitimate purposes, such as anti-

theft tracking apps, 'Find My Friends' emergency response apps, parental control apps, and others. A case manager said:

> *"It's something along the lines of "He always seems to find me." And usually when I assess, it comes down to [the victim's] location service being on the phone. I've had about three clients who had the Find My iPhone app turned on."* (P15, case manager)

Harassing and Threatening Messages and Posts

In addition to hijacking victims' devices, many participants (n=24) said that abusers who may not have access to victims' accounts frequently harass, threaten, or intimidate them via technology. In many cases, digital harassment of survivors begins, or escalates, when the abuser loses physical access to the survivor, such as when the relationship has "ended" and the survivor and abuser are no longer living together.

In its simplest form, the harassment consists of abusers calling or texting victims from their own (identifiable) devices. Survivors described how abusers would use their knowledge of survivors' lives and routines to harass them at inopportune times (e.g., at work or in the middle of the night). The harassment was also frequently persistent, with participants describing how they would receive *"upwards of 200 text messages a day; upwards of 160 calls a day."* To try and limit the harassment, many participants (n=30) said that victims often seek legal orders of protection that prevent the abuser from being able to contact them. However, abusers often respond by finding anonymous services that enable them to contact the victim via a number that cannot legally be tied to the abuser:

> *"You can put a fake number. So when you call someone, that fake number's going to come up. So they won't know it's you . . . Same thing with texting. They can text from a fake number or an online number . . . There's no way of tracking that back."* (P30, case manager)

The anonymity of these services and the plausible deniability that they afford the abuser also made it easy for the harassment and intimidation to quickly escalate, with survivors describing how their abuser would frequently threaten them, or their families, with violence or death. Despite these threats, some survivors felt it was better to accept the digital harassment than risk it turning into physical abuse:

> *"She'd rather take [the harassment] because she thinks if she reports it, she'll be in more danger. So she is accepting the violating behavior because she doesn't want to aggravate it into something more."* (P42, attorney)

Harassment via social media

In addition to calling and texting, harassment via social media was extremely prevalent, with 49 participants explicitly bringing this up. Abusers exploit a wide range of social media platforms, and one participant described how, *"Facebook is really a stalker's paradise."* Once again, the harassment often begins with the abuser posting content from their own accounts, such as Facebook statuses or Instagram photos containing threatening or derogatory comments about the victim. Although many social media platforms have mechanisms for detecting abusive content, abusers in IPV contexts frequently use their knowledge of victims to create real threats that may not be perceived as threatening by other people or detection algorithms:

> *"[The abuser] will post something on [social media], sometimes in code language . . . They'll say things that they know is a threat, but you might not think it's a threat at first if you're just looking at it."* (P24, attorney)

It is also common for abusers to create fake social media accounts from which they anonymously intimidate victims (reported by at least 18 participants). Once again, this anonymity enables abusers to continue harassing victims after being forbidden from doing so by a legal order of protection:

> *"Something that I see often is survivors being harassed by abusers through social media when there is an order of protection . . . a lot of fake Facebook profiles very obviously belong to the abuser but [the survivors] have no way to prove it. Often it's because that person writes them a message, which you can do when you're not friends with someone on Facebook."* (P1, counselor)

This quote also highlights how some features provided by different social media platforms may unwittingly aid abusers or provide information that helps to propagate the abuse. For example, as the quote suggests, it is possible to send direct Facebook messages to people one is not friends with. Similarly, WhatsApp and Viber tell the sender of a message when the message has been delivered *and* when it has been seen by the receiver. Many of these features are enabled by default and participants often did not know how to turn them off:

> *"It was WhatsApp. The survivor didn't know how to turn off the notification to the other party about whether it's read or not . . . [the abuser] would go on a rant like, "I know you read this, I know you saw it" . . . which prompted more harassment."* (P10, case manager)

Social media platforms also make it easy for abusers to involve victims' friends and family in the abuse. The abuser and victim usually share social circles and mutual friends, all of which leads to additional complications on social media. One common tactic is for the abuser to also harass the victim's friends or family, for example by messaging the victim's friends and demanding to know if they are having a sexual relationship with the victim. Alternatively, when blocked on social media by their victim, abusers try to glean information from the pages of mutual friends who are still in contact with the victim. These friends may not be aware of the abuse and unknowingly help the abuser by disclosing information about the victim. Similarly, commenting on mutual friends' social media pages enables abusers to continue to harass victims:

> *"A lot of times there's an order of protection, but if we have mutual friends and you commented on your friend's photo, I have every right to comment on your friend's photo too. I'm not talking to you, but we're on the same feed. So it gets really confusing."* (P7, case manager)

In addition to making it easy for abusers to take advantage of victims' friends and families, social media also enables abusers to recruit third parties to harass victims (reported by

12 participants). One common model is for an abuser's new intimate partner to threaten or intimidate the victim, often based on (untrue) stories that the abuser has told them:

> *"I've had survivors where people have contacted them through [social media] . . . it's like, the new girlfriend of the abuser who's threatening. So that often happens, where there are threats made by third parties, sort of as a representative of the abuser."* (P36, attorney)

Several survivors described how they found this abuse by third parties to be particularly difficult to cope with since they now did not know who the harassment was coming from and felt that they had no way to defend themselves. We also heard cases in which an abuser would use social media to manipulate different victims into being abusive towards each other:

> *"The abuser . . . was having relationships with two women and constantly had it so that they would fight over him on [social media] . . . and get them to be verbally abusive against one another."* (P49, social worker)

In trying to cope with online harassment, victims said that their attempts to have the abuser's (real or fake) social media pages shut down by service providers were unsuccessful, often for reasons they did not understand. Many participants (n=16) said that victims often felt their only option was to eventually close all social media accounts and *"go off the radar."* Unfortunately, these drastic measures may also be ineffective since, even if the victim is not on social media, the abuser is still able to post slanderous or derogatory information about them. We now discuss these exposure-based threats in detail.

Exposure of Private Information

Many participants (n=28) reported that abusers frequently use digital technologies to expose victims' private information to third parties, with the goal of humiliating, shaming, or harming the victim's reputation or endangering their relationships. One case manager described *"the stigma or what a community may think of [the victim] ... the perception of how they may be portrayed to their families and neighbors"* as the driving concern behind such harms. An abuser may threaten exposure-based harms to blackmail a victim into not reporting the abuse or not leaving the relationship; if the victim does so, exposure becomes a form of punishment and retaliation.

The most common exposure-based threat in our research was exposure of intimate images (photos or videos) of victims, commonly known as non-consensual pornography or *"revenge porn"* [45]. At least 25 participants had experience with such images. Non-consensual images may depict the victim, but may also be images of others that are described as being images of the victim. If the images do depict the victim, they may have been taken with or without the victim's consent or awareness. The abuser may expose the images to the general public, or target the exposure to specific individuals or groups with whom the victim has a special relationship and to whom such exposure will be especially harmful and humiliating, such as friends, family, colleagues, or school classmates. Social media is often used to distribute the images, either through a fake account that appears to belong to the victim or by obtaining access to the victim's real accounts:

> *". . . he shared naked pictures of me . . . he also sent them to [public media]. . . He took my phone and he sent them through private messages to friends, but he also sent them through my email and my [social media] because he had the password. ... he threatened to send them to [my work] . . . The embarrassment that I went through, the public humiliation, it ... beat me to the ground."* (P18, survivor)

In addition to intimate images, an abuser may use social media to expose (real or false) personal information about a victim to third parties. A case worker described:

> *"Say, for example ... I'm HIV positive. My partner knows, but my family doesn't know. It's like, "I'm going to go on Facebook and post that you're HIV positive . . . if you don't do what I tell you" . . . and not only Facebook, there's Instagram, Snapchat, Twitter."* (P22, case worker)

Other attacks involved publicizing a victim's personal information to facilitate abuse by others. This typically involves the abuser creating a fake profile (e.g., on Tinder) or placing an ad online that impersonates the victim, claiming that they are a prostitute and providing their address so that people come to their home to seek sexual services:

> *"He placed an ad. Those fake ads, "come rape me" style, giving her address and phone number. People went to her house . . . and she was absolutely scared. It was like one of those nightmares."* (P12, social worker)

Another case manager described a victim who had over 25 people ringing her doorbell nightly, having been sent there by the abuser to *"hook up"*. The case manager described having worked with two survivors in the last month who had been subject to such attacks. She said it could be challenging to have such ads removed, because the platforms on which they were advertised said they were *"legally paid for."*

DISCUSSION

Our findings provide a nuanced view of how abusers exploit technology to control, monitor, threaten, impersonate, and harass their victims. This section discusses broader implications of our work, beginning with how the intimate nature of the relationships in IPV cause it to differ from other forms of technology-enabled abuse. We also show how many of the attacks we saw are, from the perspective of computer security and privacy researchers, technologically unsophisticated, and in many cases can be carried out by average technology users that only interact with a system via its normal UI — what we call *UI-bound adversaries*. We then introduce the idea of IPV safety reviews for UI design, which could help address the threat of UI-bound and other adversaries. Finally, we discuss tools to help victims of IPV better understand, detect, and remove applications that may be spying on them.

Comparing IPV to Non-Intimate Technology Abuse

Our analysis shows that many of the attacks that take place in IPV contexts are in some ways similar to non-intimate technology-enabled abuse. For example, online bullying, which clearly occurs in IPV contexts, may also occur when people who don't know each other post abusive content online [2, 14]. Similarly, there have been cases where people

on the Internet reveal personal details (e.g., names and addresses) of others whom they don't know personally but with whom they disagree [15, 26]. Despite these similarities, IPV settings are often *more* complex than other contexts due to the sociotechnical and relational factors that underlie them.

Foremost among these complexities is that technology-enabled abuse intersects with other forms of abuse, including physical, emotional, financial, and others, in complex ways, owing frequently to the physical proximity, preexisting relationships, and shared social networks between the abuser and victim. At a high level, we saw that technology-enabled abuse intersected with other forms of abuse in three main ways. First, an abuser can use digital tools to enable other types of abuse—such as physically stalking someone using location data. Conversely, other forms of abuse may facilitate digital abuse—such as threatening physical harm to obtain passwords. Finally, steps taken by victims to mitigate digital abuse may have the effect of escalating other forms of abuse by a frustrated abuser.

From a security mechanism perspective, attackers in IPV use their intimate knowledge of victims to undermine the prevalent threat models on which conventional countermeasures are based. For example, our analysis shows that a key issue facing IPV victims is that their devices or accounts are often owned or configured by the abuser. Although survivors can be guided to setup new accounts that, hopefully, won't be subsequently compromised by the abuser, this may not be feasible for a variety of reasons, including when victims still live with abusers or remain financially dependent on them. In such cases, designers might conceive of new frameworks for how to think about shared devices and accounts in relationships where an abusive partner maintains control over configuration settings. A starting point may be how device sharing happens in non-IPV contexts [6, 24, 27, 29]. However, prior work on account sharing assumes that the primary user and the owner (or controller) of the account are one and the same, which is often not the case in IPV. As a result, existing countermeasures [4, 16, 23, 25, 36] may not be effective in IPV contexts.

Other examples of how IPV contexts complicate existing threat models occur on social media. As mentioned earlier, social media was called *"a stalker's paradise"* by one of our participants. Social media can be abused in a variety of contexts, and companies already laudably work to detect fake accounts, illicit content, and abusive messaging. But our data reveal that IPV presents unique and underappreciated challenges. Fake accounts may be actively used by an abuser (rather than a bot), making them more challenging to identify and label as fake. Harmful messages may not seem harmful to third parties since they exploit shared context between abuser and victim, which suggests a need for better abuse reporting mechanisms for IPV.

Attacks Require Only Basic Computing Skills

Although participants expressed fears about "hacking" and sophisticated computing knowledge of abusers, most of the attacks that came up in our data do *not* require advanced computing skills, for two reasons. First, **most attacks are technologically simple**, such as guessing a victim's password, owning the account in the first place, sending a harassing message, setting up a fake Facebook profile, etc. These widespread and very damaging behaviors do not require advanced computing skills to mount. Second, our analysis shows an **increasing commoditization of abuse tools.** The most technologically advanced threats we uncovered can be achieved using ready-made tools easily found online. Spyware is available on app stores or via a web search; GPS tracking devices can be cheaply obtained; a number of websites offer easy-to-use services for sending spoofed text messages, etc.

Although high-tech-sounding threats may capture people's attention and imagination, our data suggests that improvements will come from focusing on defending against simple-but-effective techniques easily carried out by average computer users. Unfortunately, the simplicity of abusers' attacks does not necessarily make them easy to defend against technologically, and indeed, their prosaic use of technology may even make it harder (e.g., text messages without spoofing may be less conspicuous to network operators than spoofed messages). We now detail one prevalent adversarial model that fits many of the attacks we encountered: *the UI-bound adversary*.

The UI-Bound Adversary

Our analysis shows that abusers often become *authenticated but adversarial* users of a system. Examples include compelling unlocking of a phone and inspecting the usage history or remotely accessing online accounts due to knowledge of the victim's password or security questions. In these types of attacks, the abuser has the ability (or can force the victim) to answer authentication challenges (password or PIN). From that point, the abuser interacts with the system using the same privileges as the regular user. The abuser does not seek to escalate privileges (e.g., gain root access by exploiting a system vulnerability) or use forensic tools. For this reason, we refer to such adversaries as *UI-bound*: while using the system they are bound by the functionality offered by the system's UI.

We see a number of avenues for the design of systems to better defend against UI-bound adversaries. One would be to refine authentication mechanisms to better distinguish between legitimate users and UI-bound adversaries. This might involve analyzing how the adversary's behavior when using a system differs from a legitimate user's behavior, which could be performed within cloud services (e.g., Facebook might look for common abuser behaviors and flag suspicious authenticated sessions) or within the OS of devices such as smartphones. These enhanced authentication techniques could be turned on via some mechanism outside the normal UI of the system, such as having a restricted-use portal that allows IPV professionals to help a victim turn on this extra level of monitoring.

Another approach to limiting UI-bound adversaries is to augment explicit authentication with hidden authentication mechanisms. These have been explored for non-IPV contexts in development of deniable encrypted file systems for computers [1, 3, 30] and smartphones [39]. These systems include a covert authentication mechanism hidden within a conventional authentication mechanism: enter one password to recover benign data and a different password to recover sensitive information. However, since these tools do not hide their presence on the system, it's unclear whether abusers in IPV would find their use suspicious. It's also likely that victims would find

such tools opaque and challenging to use (the average user already has a hard time understanding encryption [35,37,50], let alone deniable encryption). Moreover, usability issues would likely be exacerbated by the extreme pressures a victim is under when forced to disclose credentials.

A third approach would be for HCI researchers to create design frameworks that consider the UI-bound adversary model in the design of new systems, analyzing UIs in light of abusive users. We now discuss how this might be achieved.

IPV Safety Reviews for UI Design

HCI does not typically consider how to design interfaces that specifically *hamper* usability for some users. We suggest that new frameworks can be developed to consider adversarial users while designing and evaluating UIs in order to limit systems' abusability. Such frameworks would focus on how UI design decisions correlate with IPV victim privacy and safety and introduce new HCI concepts that might improve existing designs. Thus one would look at how to consciously *degrade* usability by adversarial users while maintaining, or minimally impacting, legitimate user experience.

A first step would be to explicitly include IPV safety reviews in the design process. Such reviews might complement other HCI audit techniques, such as finding usability problems through cognitive walkthroughs [49] or HCI heuristics [31]. We envision a methodology in which a security or privacy engineer evaluates new features from the point of view of IPV abuse scenarios, as informed by our data. One could separately consider different threat models, such as UI-bound adversaries, abusers setting up fake accounts, etc. The evaluation would involve adopting the abuser's viewpoint to explore and document avenues for harming victims. Such IPV safety reviews would therefore be a specialized form of penetration testing.

For example, consider a UI for an app or social media site that displays the user's recent physical locations on the welcome page. An abuser would clearly be able to take advantage of this information, and it may not be that relevant to regular users. Removing the feature could thus reduce the utility of the application for adversaries without substantially inconveniencing legitimate users. Even if, ultimately, companies decide that such features are still worth including, this process may result in design changes or documentation that help victims defend against such abuses (e.g., via configuration options) or, at least, allow companies to communicate the result of safety reviews with IPV advocates. Some companies have already taken steps in this direction, such as the collaboration between Facebook and the National Network to End Domestic Violence that resulted in a Facebook guide for IPV survivors [46].

Solving Spyware Mysteries

Our participants frequently mentioned the threat of spyware and suspected that abusers had installed spyware on their devices. Although many of the attacks our participants described did *not* seem to rely on installed spyware or dual-use apps, some did, and the specter of spyware installation without apparent remedy led many victims to feel that technological abuse was inevitable, unavoidable, and even provided abusers with "magical" powers (as in, "my abuser magically knows where I am"). However, despite suspecting spyware, most participants were unable to confirm whether something had been installed on their device, in part because victims and advocates lack tools for detecting such installation.

The current norm for detecting potential spyware is very circumstantial, either observing strange behavior of a device (slow responsiveness, spikes in bandwidth usage, decreased battery life), or inferring its existence because it seems the only explanation for how an abuser could possess certain information. A few victims received help by having their devices professionally assessed; however, most of the time, whether the culprit was spyware or another means of access (e.g., account ownership, device access) remained a mystery. While Google searches reveal a wide variety of software advertised as anti-spyware apps that can detect and remove spyware, no participants knew about their availability. In one focus group, participants were excited to hear from one of the authors about the concept of conventional anti-virus tools. More fundamentally it's unclear whether existing anti-virus or anti-spyware tools satisfiably flag spyware, particularly given the prevalence of dual-use apps (e.g., anti-theft or parental control apps) that can be easily repurposed to act as spyware in IPV.

A constructive next step would therefore be to systematically analyze how well existing anti-spyware tools detect both known spyware *and* dual-use apps and potentially design new tools that take into account the specificities of the IPV context. The already mentioned issue of dual-use software will complicate how to productively define what exactly constitutes "spyware" in IPV, a seemingly necessary first step towards creating effective detection tools. Even with good detection mechanisms, escalation may complicate the safe removal of spyware [21, 28], since uninstalling spyware may cut off the abuser's access to the victim in ways that trigger more severe violence. Therefore, in addition to simply removing spyware, future work could design tools that give victims more granular control, such as selectively reporting benign data.

CONCLUSION

This paper discusses how intimate partner abusers exploit technologies to intimidate, threaten, monitor, impersonate, harass, or otherwise harm their victims. We show that many prevalent attacks in IPV may be easily carried out by average technology users because traditional threat models are often undermined by the IPV context. Our analysis suggests that one important threat model in this setting is characterized by *UI-bound adversaries*, authenticated but adversarial users that interact with a system via the regular UI. We provide constructive ideas for how to deal with UI-bound and other adversaries via IPV design reviews and better tools for detecting applications used to spy on victims. Taken together, our findings set the stage for future research and improvements to IPV safety.

ACKNOWLEDGMENTS

We would like to sincerely thank all our study participants and our collaborators at the New York City OCDV and FJCs. This work was supported in part by NSF grant CNS-1330308, a Sloan fellowship, and an Engaged Cornell grant.

REFERENCES

1. 2014. TrueCrypt. (2014). http://truecrypt.sourceforge.net/.
2. Zahra Ashktorab and Jessica Vitak. 2016. Designing Cyberbullying Mitigation and Prevention Solutions through Participatory Design With Teenagers. In *ACM Conference on Human Factors in Computing Systems*. ACM, 3895–3905.
3. Julian Assange, Suelette Dreyfus, and Ralf Weinmann. 1997. Rubberhose. (1997). https://web.archive.org/web/20100915130330/http://iq.org/~proff/rubberhose.org/.
4. Jakob E Bardram. 2005. The trouble with login: On usability and computer security in ubiquitous computing. *Personal and Ubiquitous Computing* 9, 6 (2005), 357–367.
5. danah boyd. 2012. Truth, Lies, and 'Doxxing': The Real Moral of the Gawker/Reddit Story. *Wired* (2012).
6. AJ Bernheim Brush and Kori Inkpen. 2007. Yours, mine and ours? Sharing and use of technology in domestic environments. In *UbiComp*, Vol. 7. Springer, 109–126.
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 (2003), 1089–1097.
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 (2010), 251–259.
9. Victoria Clarke and Virginia Braun. 2014. Thematic analysis. In *Encyclopedia of critical psychology*. Springer, 1947–1952.
10. MR Cooley, SM Turner, and DC Beidel. 2014. Composite Abuse Scale (CAS). *Measures of Violence* (2014), 175.
11. Karen M Devries, Joelle YT Mak, Claudia Garcia-Moreno, Max Petzold, James C Child, Gail Falder, Stephen Lim, Loraine J Bacchus, Rebecca E Engell, Lisa Rosenfeld, and others. 2013. The global prevalence of intimate partner violence against women. *Science* 340, 6140 (2013), 1527–1528.
12. Gina Dillon, Rafat Hussain, Deborah Loxton, and Saifur Rahman. 2013. Mental and physical health and intimate partner violence against women: A review of the literature. *International journal of family medicine* 2013 (2013).
13. Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5 (2011), 413–421.
14. Karthik Dinakar, Birago Jones, Catherine Havasi, Henry Lieberman, and Rosalind Picard. 2012. Common sense reasoning for detection, prevention, and mitigation of cyberbullying. *ACM Transactions on Interactive Intelligent Systems (TiiS)* 2, 3 (2012), 18.
15. David M Douglas. 2016. Doxing: a conceptual analysis. *Ethics and information technology* 18, 3 (2016), 199–210.
16. Serge Egelman, AJ Brush, and Kori M Inkpen. 2008. Family accounts: a new paradigm for user accounts within the home environment. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*. ACM, 669–678.
17. Louise Ellison and Yaman Akdeniz. 1998. Cyber-stalking: the Regulation of Harassment on the Internet. *Criminal Law Review* 29 (1998), 29–48.
18. Brett Eterovic-Soric, Kim-Kwang Raymond Choo, Helen Ashman, and Sameera Mubarak. 2017. Stalking the stalkers–detecting and deterring stalking behaviours using technology: A review. *Computers & Security* 70 (2017), 278–289.
19. Marilyn Ford-Gilboe, C Nadine Wathen, Colleen Varcoe, Harriet L MacMillan, Kelly Scott-Storey, Tara Mantler, Kelsey Hegarty, and Nancy Perrin. 2016. Development of a brief measure of intimate partner violence experiences: the Composite Abuse Scale (Revised) Short Form (CAS R-SF). *BMJ open* 6, 12 (2016), e012824.
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 (2010), 39–55.
21. Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW)* Vol. 1, No. 2 (2017), Article 46.
22. Joshua Guberman, Carol Schmitz, and Libby Hemphill. 2016. Quantifying toxicity and verbal violence on Twitter. In *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing Companion*. ACM, 277–280.
23. Eiji Hayashi, Oriana Riva, Karin Strauss, AJ Brush, and Stuart Schechter. 2012. Goldilocks and the two mobile devices: Going beyond all-or-nothing access to a device's applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2.
24. Amy Karlson, AJ Brush, and Stuart Schechter. 2009. Can I borrow your phone?: Understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1647–1650.

25. Yunxin Liu, Ahmad Rahmati, Yuanhe Huang, Hyukjae Jang, Lin Zhong, Yongguang Zhang, and Shensheng Zhang. 2009. xShare: Supporting impromptu sharing of mobile phones. In *Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services*. ACM, 15–28.
26. David W Macdonald, Kim S Jacobsen, Dawn Burnham, Paul J Johnson, and Andrew J Loveridge. 2016. Cecil: a moment or a movement? Analysis of media coverage of the death of a lion, Panthera leo. *Animals* 6, 5 (2016), 26.
27. Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. She'll just grab any device that's closer: A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 5921–5932.
28. Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2189–2201.
29. Michelle Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Cranor, Gregory Ganger, and Michael Reiter. 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)*. ACM, New York, NY, USA, 645–654.
30. Andrew D McDonald and Markus G Kuhn. 1999. StegFS: A steganographic file system for Linux. In *International Workshop on Information Hiding*. Springer, 463–477.
31. Jakob Nielsen. 1992. Finding usability problems through heuristic evaluation. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 373–380.
32. Shirley Patton. 2003. Pathways: How women leave violent men. (2003).
33. Ellen Pence and Michael Paymar. 1990. *Power and control: Tactics of men who batter: An educational curriculum*. Minnesota Program Development Incorporated.
34. Rebecca F Rabin, Jacky M Jennings, Jacquelyn C Campbell, and Megan H Bair-Merritt. 2009. Intimate partner violence screening tools: a systematic review. *American journal of preventive medicine* 36, 5 (2009), 439–445.
35. Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. 2015. Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *arXiv preprint arXiv:1510.08555* (2015).
36. Julian Seifert, Alexander De Luca, Bettina Conradi, and Heinrich Hussmann. 2010. Treasurephone: Context-sensitive user data protection on mobile phones. *Pervasive Computing* (2010), 130–137.
37. Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. 2006. Why Johnny still can't encrypt: Evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*. 3–4.
38. Aily Shimizu. 2013. Domestic violence in the digital age: Towards the creation of a comprehensive cyberstalking statute. *Berkeley J. Gender L. & Just.* 28 (2013), 116.
39. Adam Skillen and Mohammad Mannan. 2014. Mobiflage: Deniable storage encryption for mobile devices. *IEEE Transactions on Dependable and Secure Computing* 11, 3 (2014), 224–237.
40. Sharon G Smith, Kathleen C Basile, Leah K Gilbert, Melissa T Merrick, Nimesh Patel, Margie Walling, and Anurag Jain. 2017. National Intimate Partner and Sexual Violence Survey (NISVS): 2010-2012 state report. (2017).
41. 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* (2005).
42. Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. Intimate partner violence, technology, and stalking. *Violence against women* 13, 8 (2007), 842–856.
43. Cindy Southworth and Sarah Tucker. 2006. Technology, stalking and domestic violence victims. *Miss. LJ* 76 (2006), 667.
44. Heidi Stöckl, Karen Devries, Alexandra Rotstein, Naeemah Abrahams, Jacquelyn Campbell, Charlotte Watts, and Claudia Garcia Moreno. 2013. The global prevalence of intimate partner homicide: a systematic review. *The Lancet* 382, 9895 (2013), 859–865.
45. Scott R Stroud. 2014. The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *Journal of Mass Media Ethics* 29, 3 (2014), 168–183.
46. National Network to End Domestic Violence and Facebook. 2014. Privacy & Safety on Facebook: A Guide for Survivors of Abuse. (2014). `http://nnedv.org/downloads/SafetyNet/NNEDV_FB_Privacy_and_Safety_Guide_2014.pdf`.
47. Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab. 2017. Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment. In *ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, 1231–1245.
48. Lenore E Walker. 1977. Battered women and learned helplessness. *Victimology* (1977).

49. Cathleen Wharton, John Rieman, Clayton Lewis, and Peter Polson. 1994. The cognitive walkthrough method: A practitioner's guide. In *Usability inspection methods*. John Wiley & Sons, Inc., 105–140.

50. Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, Vol. 348.

51. Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F Perkins, and John M Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 3919–3930.

52. Delanie Woodlock. 2016. The abuse of technology in domestic violence and stalking. *Violence against women* (2016), 1077801216646277.

53. Kersti A Yllo. 2005. Through a feminist lens. *Current controversies in family violence* (2005).