Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders

DIANA FREED, Information Science, Cornell Tech, USA
JACKELINE PALMER, Hunter College, USA
DIANA MINCHALA, City College of New York, USA
KAREN LEVY, Information Science, Cornell University, USA
THOMAS RISTENPART, Computer Science, Cornell Tech, USA
NICOLA DELL, Information Science, Jacobs Technion-Cornell Institute, Cornell Tech, USA

Digital technologies, including mobile devices, cloud computing services, and social networks, play a nuanced role in intimate partner violence (IPV) settings, including domestic abuse, stalking, and surveillance of victims by abusive partners. However, the interactions among victims of IPV, abusers, law enforcement, counselors, and others — and the roles that digital technologies play in these interactions — are poorly understood. We present a qualitative study that analyzes the role of digital technologies in the IPV ecosystem in New York City. Findings from semi-structured interviews with 40 IPV professionals and nine focus groups with 32 survivors of IPV reveal a complex set of socio-technical challenges that stem from the intimate nature of the relationships involved and the complexities of managing shared social circles. Both IPV professionals and survivors feel that they do not possess adequate expertise to be able to identify or cope with technology-enabled IPV, and there are currently insufficient best practices to help them deal with abuse via technology. We also reveal a number of tensions and trade-offs in negotiating technology's role in social support and legal procedures. Taken together, our findings contribute a nuanced understanding of technology's role in the IPV ecosystem and yield recommendations for HCI and technology experts interested in aiding victims of abuse.

CCS Concepts: • **Security and privacy** → *Social aspects of security and privacy*;

Additional Key Words and Phrases: IPV; intimate partner violence; domestic violence; violence against women; domestic abuse; privacy; safety; security.

ACM Reference Format:
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. *Proc. ACM Hum.-Comput. Interact.* 1, 1, Article 46 (September 2017), 22 pages.
https://doi.org/10.1145/3134681

1 INTRODUCTION

Intimate partner violence (IPV) is a pervasive problem that affects roughly one-third of all women and one-quarter of all men [5], with one in five women and one in seven men experiencing severe physical violence by an intimate partner at some point in their lifetime [37]. As digital technologies play an increasingly central role in our everyday lives, its role in IPV is also increasing. Prior research indicates that abusers commonly use technology to exert control over victims, including

2573-0142/2017/9-ART46
https://doi.org/10.1145/3134681

physical stalking facilitated by access to digital location services [33], virtual stalking by remotely accessing cameras on victim devices [31], monitoring of victim contacts on social networks and email [11], and tracking by way of surreptitiously installed spyware on victim devices [24]. Recent work by Matthews et al. [26] shares reports by victims of such abuses, and points out specific tensions that arise in trying to design technologies that provide better safety and privacy.

All of this work, however, focuses on the interactions between a victim and an abuser and/or specific modes of technology-enabled abuse. But in trying to cope with IPV situations, survivors often draw on support provided by a broad ecosystem of stakeholders, including their family and friends, counseling and social support networks, law enforcement, legal services, and others. To date there has been no investigation of how technology issues impact this broader set of stakeholders, and how that affects privacy and safety for victims.

We fill this gap by contributing a qualitative study that examines the role of technology in the IPV ecosystem in New York City (NYC). We partnered with the Mayor's Office to Combat Domestic Violence (OCDV), which runs Family Justice Centers (FJCs) in the five boroughs of NYC. The FJCs provide survivors of IPV with free and confidential civil, legal, and supportive services, and each FJC houses representatives from a range of organizations to make it easy for survivors to get help in one location. Representatives include those from key city agencies, non-profit and community organizations, social and civil legal services providers, law enforcement, and district attorneys.

We conducted semi-structured interviews with 40 professionals that work at the FJCs and nine focus groups with 32 survivors of IPV who were clients at the FJCs. Our data provides us with a broad view of the different stakeholder groups and how they interact to provide survivors with legal and social support services. We then present an analysis of the multifaceted and often nuanced role that technology plays in the IPV ecosystem. We uncover a complex set of socio-technical challenges that emanate from the intimate nature of the relationships involved and the physical and digital complexities associated with managing shared families and social circles. As one example, use of privacy controls to block abusers on social media or phones can escalate abuse from online harassment to physical violence. A frequent recommendation by professionals to stop using specific technologies can improve privacy but prevents victims from accessing social support or economic opportunities. Although professionals are aware of these tensions, our findings suggest that there are currently insufficient best practices to help them help survivors.

The lack of best practices also puts pressure on professionals and, in turn, survivors, to develop ad-hoc strategies for digital privacy and safety. Simultaneously, both professionals and survivors feel that they do not possess adequate knowledge or expertise to be able to identify or cope with IPV-related technology issues. Professionals will *"Google-as-they-go"*, i.e., search the web for information on technology during meetings with survivors, or will ask co-workers if they have experience with technologies. A final set of issues arise at the intersection of the law and technology. Survivors and legal professionals must collect digital evidence to prove IPV in court so that they can prosecute offenders and/or obtain legal orders of protection. This is made complex by the struggle of laws and forensic procedures to keep up with the pace of technology change, and also by the fact that evidence collection can frequently conflict with victim privacy needs.

Our analysis has implications for the design of technological interventions that target IPV settings. Clearly, technologists need to take into account the subtle tensions that arise in IPV, such as between privacy and escalation. Perhaps less obvious is that intervention design could be more successful by explicitly considering the many stakeholders in the IPV ecosystem beyond just the victim and abuser. For example, future work could explore co-designing new privacy controls for social media and other technologies, in parallel with new procedures and materials for IPV professionals. This could better enable professionals as they strive to provide survivors with social support and legal services.

2 RELATED WORK

2.1 Studies of the IPV Ecosystem

There is a long line of work on non-technological aspects of IPV, focusing on legal, health, and psychological issues, and on the ecosystem of stakeholders involved. IPV has been discussed in terms of cycles and phases that capture survivors' experiences including physical, emotional, and psychological abuse [7, 39]. It is widely documented that survivors of IPV have a difficult time leaving abusers, and Patton et al. [29] identified factors contributing to this difficulty. A chief concern is the safety of the survivor as they move away from the abuser and the potential for subsequent escalation of violence by the abuser in a quest for control [14, 22]. Our results suggest that technology plays an intimate, complicating role when leaving an abusive relationship and that technology plays both a positive and negative role in escalation.

In terms of the ecosystem, prior work has investigated the role of (general) health care professionals in screening for IPV [27, 30]. Many victims of IPV first present to health care professionals, and the consensus seems to be that standard practices to spot signs of abuse during health care visits would allow for earlier interventions [17]. Unfortunately adoption of this viewpoint has been slow [2, 16, 36, 38]. Other work has focused on how to improve the ecosystem of professionals in order to improve outcomes. For example, prior work showed that integrating social services into the criminal justice system may enable better response to the needs of survivors [15, 43]. Related work demonstrates the importance of addressing the needs of front-line providers and service infrastructures in designing systems for other vulnerable groups [23, 41]. Victims of IPV face unique legal challenges because the offender is known to them, and the literature shows inconsistent findings in terms of the efficacy of criminal justice and civil solutions [19]. Our results suggest further complications in legal processes due to the role of technology in IPV.

2.2 Technology and IPV

Prior work has highlighted the use of technology to abuse. A lot of attention has been given to online harassment, cyberstalking, and cyberbullying [12, 14, 28, 33], specifically in adolescent and youth populations [4, 21]. While sharing some similarities with IPV, these forms of abuse lack the distinctive, complicating existence of an intimate relationship between victim and abuser.

In the IPV context, previous work has pointed out various ways abusers make malicious use of technology [33]. Abusers exploit location-based services, phone records, social media, shared online banking, hidden cameras, and spyware to track and exert control over a victim [14, 33]. Exacerbating this is the fact that abusers in the IPV context may be able to infer, or compel disclosure of, authentication credentials, thereby gaining access to victim accounts and devices. In addition to tracking and control, intimate partners can use technology to harass the victim. Examples include posting non-consensual pornography, *"doxing"* the victim (making public private information), or sending abusive messages or pictures, sometimes from fake phone numbers or accounts. (The latter is often referred to as spoofing.) We encountered examples of all of these abuses in our research.

Previous work has shown the usability challenges of privacy and security tools [10, 18, 20, 40], which can be even more severe for victims of IPV due to their extreme threat model [25, 26]. There exist a few online resources for survivors to increase their privacy and security, most notably the National Network to End Domestic Violence (NNEDV) maintains technology guides for social media, mobile phones, and more. Nevertheless, our study suggests that existing guides are often insufficient to help professionals and survivors.

Arief et al. [3] lay out a vision for *"sensible privacy"* design that considers both victim needs and the potential for abuse. They also sketch the design of an app that would erase information about visits to IPV-relevant websites by a user, while also recording potential abuse of the device.

Similarly Emms et al. [13] suggest tools for helping survivors erase their browser history. A number of other apps for survivors have been proposed, including NNEDV's TechSafety app [35], the Safe Chat Silicon Valley app [32], and others. These attempt to provide victims with resources, such as for safety planning [28].

Closest to our work is previous interview-based studies of IPV and technology. Dimond et al. [11] interviewed ten female survivors about their technology and shared example stories. They report on victims' abuse via social networking and mobile phones, their challenges managing privacy settings, and the fact that victims often feel less technologically savvy than their abuser. Matthews et al. [26] interviewed 15 survivors of IPV about privacy and security. They formulate a three-stage model (physical control, escape, and life apart) to reason about technology issues and how they differ at different stages of IPV. Our work is broader, providing perspective on the larger IPV ecosystem, in particular via interviews with IPV professionals and survivors. Woodlock [42] used surveys to interview both professionals and victims, but focused on abuser tactics. Our work offers a broader view, including the way professionals and victims interact with respect to technology.

3 STUDY DESIGN

The goal of our research is to develop a nuanced understanding of the role played by digital technologies in the IPV ecosystem. To achieve this goal, we conducted a qualitative study in partnership with the New York City Mayor's Office to Combat Domestic Violence (OCDV)[1]. The OCDV in New York runs several Family Justice Centers (FJCs)[2] that provide survivors of domestic violence with free and confidential civil, legal, counseling, and supportive services. Each FJC houses representatives from key city agencies, non-profit and community organizations, social and civil legal services providers, and NYC law enforcement and District Attorney's offices.

Our research took place at four FJCs located in socioeconomically diverse neighborhoods in NYC. Specifically, we conducted one-on-one semi-structured interviews with 40 professionals who work at the FJCs and focus groups with 32 survivors of IPV who visit the FJCs to receive services and support. We use the term *"professional"* to refer to participants whose job involves working in the IPV ecosystem, including case workers, social workers, attorneys, law enforcement, and others, as described below. We use the term *"client"* to refer to participants who are survivors of IPV, including people who are still living with their abuser and those who have left the abusive relationship; *"client"* is the term used by FJC professionals for people who make use of their services. The rest of this section describes our methods in detail. We received IRB approval for all study procedures and permission from the OCDV before beginning our research.

3.1 Recruitment

We recruited 72 participants (40 professionals and 32 clients) at four FJCs. Before recruiting participants we spoke with the Deputy Director at each FJC to explain the purpose of our research and request their assistance. To recruit professionals, the Deputy Director helped us by making a wide range of professionals aware of the opportunity to participate in our study. Interested professionals then contacted the Deputy Director who helped us to schedule one-on-one interviews. To recruit clients, the Deputy Director placed fliers (in English and Spanish) that described the study in the FJC reception area. The fliers instructed clients who were interested in participating to contact the Deputy Director, who then assisted with the formation and scheduling of the client focus groups.

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

40 professionals		
Gender	Female: 35 Male: 5	
Age (yrs)	Min: 22 Max: 56 Average: 33	
Research sites	FJC A: 7 FJC B: 12 FJC C: 11 FJC D: 10	
Professional Role	Case manager/case worker:	16
	Social worker	10
	Attorneys/paralegals	8
	Police officers	6

32 clients			
Gender	Female: 32 Male: 0		
Age (yrs)	Min: 25 Max: 55 Average: 35		
Countries of origin	Argentina, Dominican Republic, Ecuador, Egypt, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Peru, Russia, UK, USA		
Research sites		English	Spanish
	FJC A:	6	0
	FJC B:	2	6
	FJC C:	4	10
	FJC D:	0	4
Education	Did not complete high school:		5
	Completed high school:		10
	Attended college, did not graduate:		5
	Completed college:		7
	Unreported:		5

Fig. 1. Summary of participant demographic characteristics.

3.2 Semi-Structured Interviews with Professionals

We conducted 30-minute interviews with 40 professionals working in the IPV ecosystem. Figure 1 provides some participant demographic characteristics. After explaining the study procedures and purpose of our research, we obtained written informed consent from all participants. All interviews were conducted in English at the FJC offices. The interviews were semi-structured and guided by a list of topics. We asked questions that sought an understanding of participants' demographics, their role in the IPV ecosystem, professional background and experience working in IPV, level of comfort and expertise with technology, different forms of technology-enabled abuse that they have encountered, and other ways in which technology may have come up in their work.

The first author conducted all the interviews with another team member present to take notes. All but one of the interviews were audio-recorded with permission from participants and transcribed prior to analysis. One participant did not feel comfortable being audio recorded and we captured this interview through detailed handwritten notes. At the suggestion of the OCDV, we did not compensate the professional participants.

3.3 Focus Groups with Clients

We conducted nine focus groups with 32 survivors of IPV who were clients at the FJCs (see Figure 1). We chose to talk to clients in groups because the OCDV advised us that they would be more comfortable in a group setting, be more willing to share experiences, and may benefit from hearing stories told by fellow clients. The focus groups took place on site at the FJCs and, at the suggestion of the OCDV, we provided food and gave each participant $10 as compensation for their time. Each focus group lasted 60-90 minutes and ranged in size from one to ten participants (one participant elected to speak with us alone instead of in a group). Since many of the clients speak Spanish, we held focus groups in both English (6 focus groups) and Spanish (3 focus 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). The

clients responded in Spanish and their answers were translated into English. All focus groups were audio-recorded with permission from participants and transcribed prior to analysis.

The focus groups were guided by a list of topics. We asked participants what digital devices, applications, and services they use, if technology plays a role in their abusive relationship, strategies for protecting themselves, technology advice or assistance they have received, and their ideas for what might help when it comes to technology. We reminded participants that they were not required to answer any questions and were able to leave at any time. We also took a number of steps to protect participant safety and privacy. For example, we did not require participants to sign a consent form since we did not want to record any identifying information (e.g., their names). In addition, although we provided a printout of the study information that participants could keep, we pointed out that if they took the printout home somebody may see it and learn about the focus group. Finally, an experienced IPV case worker was available at all times to speak with participants and/or researchers to help them process any upsetting experiences that may have occurred as a result of the group discussions.

3.4 Data Analysis

Our interviews and focus groups resulted in 32 hours of audio recordings that were transcribed into 812 pages of transcripts. We analyzed our data inductively [34], beginning with a close reading of the transcripts and allowing codes to emerge from the data. Our initial pass through the data resulted in approximately 70 distinct codes (for example, *abuser device access*, *digital evidence*, *desire for training*, and *threw away device*). Related codes were clustered into high-level themes. The codes and themes were discussed by the team, iteratively refined, and codified in a codebook. Three team members used the codebook to analyze a small subset of the transcripts with the goal of ensuring that the codes were sufficiently well-defined and comprehensively represented the data. Following this, one researcher coded the remaining interview data and another the focus group data.

3.5 Ethics and Anonymity

We are committed to ensuring that the benefits of our work outweigh the risks to participants. In reporting findings, we have taken steps to ensure anonymity of clients. All stories and quotes are intended to be generic accounts of issues that came up frequently. In some cases, we have slightly altered the phrasing of quotes to remove potentially unique word choices. Where possible, we use professionals' general descriptions of abusive situations rather than specific client experiences. We were also concerned that our findings should not teach abusers new methods of abuse. All of the abuse strategies that we describe came up many times throughout our data and, as our findings show, abusers are already frequently using the Internet to learn such strategies. Finally, many participants wanted their stories to be heard in the hope that technologists would be motivated to engage with IPV or that their experiences may help others affected by IPV. As one client said,

> *"The reason that I came today is because I'm hoping to let people know my story. Maybe this is going to help somehow, to help another person who is going through the same thing."* (P23, Client)

4 THE IPV ECOSYSTEM

Before analyzing the role of technology, we need to understand the various stakeholders involved in the IPV ecosystem and how they interact to provide clients with social support and legal services. Figure 2 summarizes the services that are offered to clients at the FJCs and depicts the typical movement of clients through the system. Most clients were referred to the FJCs through police officers or hospital staff after being assaulted by an abusive partner. Through conversations with

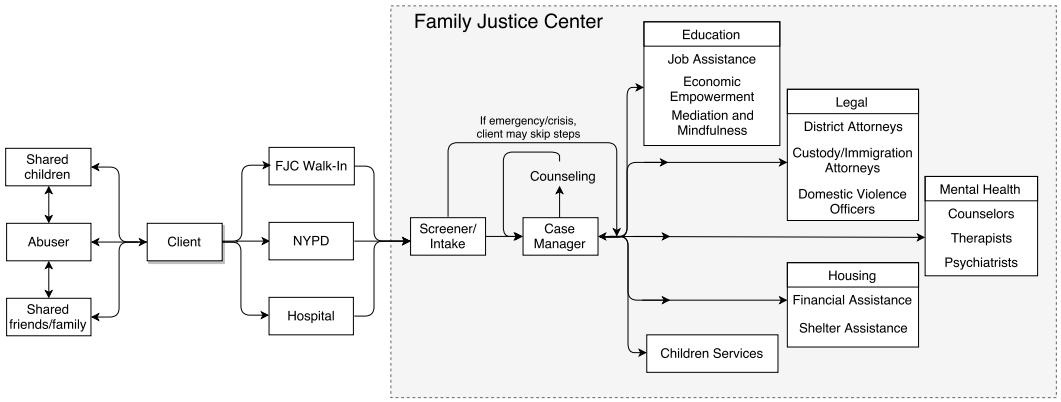

Fig. 2. Summary of the IPV ecosystem and typical paths that clients take as they navigate the services offered by the Family Justice Centers.

law enforcement, we learned that police officers usually refer clients to the FJC whenever they respond to a domestic violence call, regardless of if the client is planning to leave the abuser. Clients described enduring repeated emotional and physical abuse that frequently resulted in calls to the police, with and without hospitalization and referrals to the FJC. In addition to referrals, the FJCs also get walk-in clients seeking only legal services, counseling, or general assistance.

The first time a client visits the FJC they meet with a screener, who completes an initial assessment to determine which FJC services could be beneficial. The screener then assigns the client to a case manager for a same-day visit and connects them with legal services (if needed), with the goal of getting the client support quickly. The case manager works with that client for the duration of their interaction with the FJC. The case manager begins with a detailed assessment of the client's situation, including safety planning procedures and determining appropriate resources and referrals for the client. There are representatives from over 23 different agencies and organizations housed within the FJC system that provide a diverse range of services, including housing and shelter assistance, financial education, child services, job preparedness, and more. Clients are welcome to attend workshops as needed and decide how they would like to participate. There is one centralized initial assessment form utilized by all of the FJC's, after which each organization uses their own assessment form, although we did not come across any forms that asked about technology. It is also worth noting that information is not formally shared between the various agencies. For example, case workers do not share client case files with legal professionals, and vice versa.

From a law enforcement perspective, each FJC houses several dedicated Domestic Violence (DV) police officers, who see clients and act as a liaison between caseworkers, district attorneys, and other police officers at local precincts. If a client describes a possible crime, DV officers take a report and forward it to the relevant local precinct. Officers from that precinct follow up by conducting home visits, making arrests, or closing the case. Frequently, clients at the FJC already have active cases in which the abuser has been arrested and the client given a legal order of protection. Should the abuser violate the order by contacting the client, DV officers at the FJC take steps to have the abuser rearrested.

In addition to interacting with case workers and the police, clients who need legal services are assigned to an attorney within the FJC. Depending on the client's situation, they may see an attorney that specializes in immigration, housing, or family/custody issues, in addition to district

attorneys who prosecute criminal cases. There are also specialist services for children who are victims of domestic violence or who have witnessed domestic violence in their home.

Although there are many different organizations and numerous stakeholders housed at the FJCs, our participants described how this organizational diversity was perhaps the biggest strength of the model. Professionals are able to communicate and learn from one another as they strive to provide services that help their clients through extremely difficult situations, while clients are able to access many of the services that they need in a single location. One participant told us,

> *"I think that's why the Family Justice Centers have such a good foundation for a model that is useful and sustainable and really kind of holistic in the way that it works with people on a multitude of issues . . . to have one space where people can come and see multiple service providers in one day is very useful."* (P31, Case manager)

5 THE ROLE OF TECHNOLOGY IN THE IPV ECOSYSTEM

Armed with a nuanced view of the IPV ecosystem in NYC and a deeper understanding of the interactions between stakeholder groups, we now explore the role of technology. Our findings are organized into five major themes: (1) revealing socio-technical factors that complicate the IPV ecosystem; (2) discussing clients' knowledge and understanding of technology; (3) describing professionals' expertise and strategies for learning about technology; (4) explaining what technology-related advice and assistance clients receive at the FJCs; and (5) highlighting challenges, constraints, and trade-offs when it comes to technology, the law, and legal procedures.

5.1 Socio-Technical Complexities in the IPV Ecosystem

Our findings reveal a complex set of socio-technical issues that shape the role played by technology in the IPV ecosystem. For example, the intimate nature of the relationships involved mean that abusers are often able to gain access to the client's digital accounts and devices and use them to exert control over the client. In addition, shared social circles, children, and extended families often make it difficult or impossible for a client to truly *"escape"* from the abuser in either the physical or the digital world. Finally, technology plays a role in commoditizing abuse by helping abusers to locate, harass, and hurt victims. We discuss each of these issues in turn.

5.1.1 Intimate relationships complicate digital privacy. One of the biggest digital security and privacy challenges in IPV situations stems from the fact that the client and abuser have shared an intimate, in-person relationship and, as a result, the abuser is frequently able to gain access to the client's devices and online accounts. A case manager described,

> *"Using technology is the fastest and easiest way, I think, for many of our clients' abusers to gain access, because it's so easy — when you've been cohabitating with somebody for so long — to gain access to bank accounts, social security numbers, all of these things via shared devices, phones, and things like that. Many of our clients have to sort of untangle that, as well as figure out which accounts have been compromised."* (P31, Case manager)

In some cases, clients had willingly shared passwords with their abuser when the relationship was still good, often describing that they *"didn't have anything to hide"*. Others said that they were forced to hand over their device and/or share their passwords, with several describing that the abuser gave them *"no choice"*. In many cases, taking the device away from the client was an abusive tactic used to hurt or control the client. Another common strategy was for the abuser to go through the client's phone when they were not looking, such as while they were asleep or taking a shower. Regardless of how the abuser gained access, many clients reported having *"no idea"* what the abuser may have done on their device.

Even after physically leaving the relationship, many clients reported that their abusers were able to *"hack"* their online accounts by correctly answering the security questions and resetting the account password. A police officer described,

> *"A lot of clients tell me that he keeps getting their password to their Facebook. I tell them it's because he knows all your information. It's easy to get into your password if you know the security questions to answer."* (P27, NYPD)

Another complexity that came up frequently was that of cellular account ownership. Many clients reported sharing a cellular family plan, with their abuser as the account manager for the plan. In this situation, the abuser is in fact the legal owner of the client's account (and any children's accounts) and can track the devices using anti-theft software, activate or deactivate services, and view billing information containing details of any calls, texts, or charges made to the account. Furthermore, since many clients were financially dependent on the abuser, they often felt unable to cancel the family plan, particularly if doing so would mean purchasing new devices and cellular plans for themselves and their children.

The relationships involved in IPV often mean that a client and abuser have children together, which adds additional complexity with respect to technology use. A client shared,

> *"He gave my child an iPad and was using that to find out what's going on at home. He would use Facetime, where he gets to see where my child is and maybe what's going on in the background. It's like having him at home again, even though he's not actually there."* (P24, Client)

This story is a good example of the social complexities that frequently manifest in the IPV ecosystem. On one hand, as the parent of the child, the abuser has a clear interest in seeing and interacting with them using digital technologies; the child also has an interest in interacting and building relationships with both parents. On the other hand, it is very easy for the child and their device to become tools that are used by the abuser to continue to harass, stalk, and control the client. Trying to effectively manage these tensions frequently causes additional fear, stress, and anxiety for clients; even after they have managed to physically leave the abusive relationship, disentangling oneself *digitally* is much more difficult.

5.1.2 Shared social circles make it challenging to 'delete' the abuser. As discussed above, the intimacy and longevity of many abusive relationships result in complex social entanglements that often involve shared children, extended families, and groups of mutual and/or separate friends. These entanglements often make it extremely difficult or impossible for a client to ever truly *"escape"* from an abuser, both in the physical world and in the digital world. An attorney described,

> *"Especially in intimate partner cases, there is a lot of overlap in people's social circles. A lot of family overlap, especially if there are children in common. So now with social media you get a lot of influence being put on people. For example, now the abuser's family is posting on Facebook, 'Why'd you get my brother locked up? Why'd you get my son locked up?' "* (P28, Attorney)

Clients frequently have a hard time preventing and/or managing these kinds of unwanted interactions because they often do not know how to manage the different privacy settings associated with each social computing platform. Understanding exactly who is able to see their profile, pictures, and information, as well as who is able to comment on their posts or post on their Facebook page is challenging and requires a nuanced understanding of privacy settings. As one client told us,

> *"I try to make sure that when I post it is only seen by my friends, but I realized that there is also a setting where it could be seen by friends of friends. I want to turn that off but I do not know how."* (P9, Client)

Abusers frequently turn to mutual friends to try and obtain information about the client and, if the abuse is private and the friend is unaware, they often unknowingly aid the abuser by providing details about the client. On the other hand, abuse that becomes public knowledge via social media platforms can be devastating for clients. A case manager said,

> *"On social media, the victimization goes above and beyond the walls [of an apartment] to outsiders, strangers, and family members. And it's really hard to dispute what's being said in those public places. People like to hear gossip and are curious . . . that's something that pains a victim very long term."* (P3, Case manager)

Moreover, the burden of blocking or deleting the abuser, their family members, and any mutual friends is usually on the client. Several professionals described how they have experienced cases where a client has chosen to trust the *"wrong person"* who has gone on to provide the abuser with information that compromised the client's privacy and safety.

5.1.3 Technology can commoditize abuse. Modern digital technologies make the world's information available at the touch of a few buttons. However, in the hands of an abuser, such informational power can easily be used to harass and hurt others, with simple Internet searches yielding a vast amount of information on how to abuse—and providing access to tools that facilitate abuse. An attorney described,

> *"It is hard because with the Internet, suddenly lots of people who have the time to invest in Google searches can become very proficient very quickly using technology for not great ends. A lot of people are able to quickly school themselves on how to monitor other people if that is what they want to do. Until it happens to you, I don't think it occurs to you to be on the lookout for the signs of it. Like, my phone is very hot, the battery disappears constantly. They think, 'Well, I just need a new phone'. No. Probably someone has spyware on your phone, but you don't know that."* (P28, Attorney).

As this participant points out, there are many spyware and/or tracking apps that anyone can download, many of them available on official app stores. Moreover, in addition to apps that are specifically intended to facilitate abuse, there are also dozens of legitimate apps that can be misused by abusers. One prevalent category of apps that came up a lot in our data were tracking apps, ranging from child-monitoring apps for parents to anti-theft apps like *Find my iPhone*, all of which are commonly used by abusers to monitor clients.

In addition to enabling abusers to search for information on how to abuse, the Internet also enables abusers to find information that can help them locate a victim. Personal and organizational websites, blogs, social media platforms, and more, often provide names, photos, contact information, and other details. Once a person has an established online presence, it can be extremely difficult to remove all of their information from the Internet. Moreover, even after physically escaping an abusive relationship, clients described how starting a new life would often require them to post information online that may put them at risk. Several clients discussed how the organizations that they worked for used social media platforms to post job-relevant information that they were required to follow. Others described how the job-search process required them to create online profiles. One client shared,

> *With the employment boards . . . there's just so many of them where you have to fill out these online profiles. And whenever I'm doing a profile, kind of half of my information is true and half of it isn't.* (P2, Client)

5.2 Client understanding and knowledge of technology

Our client participants came from diverse educational and socioeconomic backgrounds and had different levels of experience with technology. Despite these variations, many (n=18) clients explicitly described themselves as lacking in technology expertise. For example, several participants said that they had *"zero knowledge"* when it comes to technology. Others described how they had *"no idea"* how to do things like turn off location services, manage privacy settings, or set up new accounts. One particularly common theme in our analysis was a lack of client understanding about if or how technology was playing a role in their abuse. Frequently, this topic manifested through stories in which, although technology-enabled abuse was the most likely explanation for something, the client had no idea that this was the case. An advocate described,

> *"There have been instances where clients can't figure out, "How is he finding me? Every time I go to this place, he's there. Every time I'm walking here, how does he know? He shows up." ... I think most people who come in — especially if they're a little bit older, maybe in their mid-30s to 40s — they aren't aware of what our phones can do."* (P34, Victim advocate)

In these situations, it is usually up to the professional to infer from the client's description of their experience that technology is likely being used as a tool for abuse, which may or may not happen depending on the professional (we discuss professionals' technology expertise below).

In addition to describing their own lack of technical expertise, both clients and professionals said that it was common for the abuser to be *"more tech-savvy"* than the client. In many cases, the abuser had purchased all the digital devices for the family and set them up in the home. This frequently gave the abuser additional power over the client during the relationship, such as changing the device's settings or controlling the client's computer. Further, being the one who set up the client's accounts also made it easier for the abuser to gain access to those accounts for abusive purposes. As one case worker said,

> *"She's absolutely not savvy on technology. I don't doubt he has access to her accounts and the passwords and everything because she never set those things up. He set those things up."* (P12, Case manager)

5.2.1 Technology-enabled abuse leads to fear of technology. As described above, many clients feel that they do not possess sufficient knowledge when it comes to technology which, when combined with the fact that technology has been used to abuse them, often results in clients being fearful of and lacking trust in *all* technology. One client told us, *"I closed everything. I'm so scared of software."* Another, upon discovering some of Google's built-in location services, described,

> *"[Google is] just trying to track me ... Literally I can go back for months and see where I was at. I had to disable everything. I would not even put information in my phone for a Google account. I'm back to using a paper calendar."* (P2, Client)

As this participant suggests, one common strategy is for clients to do their best to avoid technology altogether and shut down everything. However, as we discussed above, completely avoiding technology may be difficult or impossible, especially if the client needs to use technology to look for employment or register for services. Therefore, an alternative strategy is for clients to try and learn more about technology in the hope of being able to better protect themselves.

5.2.2 Clients want to learn about technology. Clients described different strategies for learning about technology, including taking the initiative to educate themselves through Internet searches and seeking advice from IPV professionals. Unfortunately, many clients expressed frustration at how challenging it was to learn how to protect themselves with respect to technology, describing how

they would spend hours searching for information on Google, but *"get nowhere"*. Many participants (n=15) expressed an explicit desire for better tools and trainings to increase their awareness and education about technology and, in our nine focus groups, clients asked us over 75 questions, ranging from general tech questions such as, *"If you uninstall an app, does it still have access to your data?"*, to abuse-related questions such as, *"If I turn off my phone, does [find my iPhone] still work?"* Although we repeated many times that we were there to learn from the clients and not teach them about technology, several clients said that they found the focus groups helpful. One said,

> *"We know you're not teaching us stuff. We're aware of that, but what you're doing is you're helping. Making us aware and highlighting things that we may not have known, or I didn't know."* (P3, Client)

Finally, although there are currently several apps available on official app stores that have been designed for IPV victims, none of our participants used such an app. Unsurprisingly, clients frequently turned to the various professionals working in the IPV ecosystem for help and advice.

5.3 Professional expertise and knowledge of technology

Although professionals had varying levels of expertise and experience with technology, we did not come across anyone with formal education or extensive work experience in a technology-related field. Regardless of professional role, most (n=24) participants said that they lacked sufficient technology expertise to help clients. One attorney said,

> *"I think there's so much out there, but we don't even know what can be done, and sometimes we don't know what questions to ask. I wouldn't be asking questions because I wouldn't know that those are questions I should be asking. And if the client isn't aware or doesn't know how to explain it to me or doesn't bring it up, it might not be something that we address."* (P14, Staff attorney)

Ten professionals also mentioned that they have difficulty keeping up with the rapid pace of technology change. There are currently few formal avenues for professionals to learn about client technology issues, and the onus is often on the individual to take the initiative and seek out more information. Frequently mentioned strategies include searching the Internet for information and asking colleagues who may have had clients with similar issues, as we now discuss.

5.3.1 Professionals "Google-as-they-go". A common strategy for learning about technology was simply searching the web for information during or between client meetings. This could be both for general technology information, such as learning about new apps, or for digital privacy/safety specific problems, such as how to prevent location tracking. A case manager said,

> *"I end up Googling it. And then I'll deal with the issue. I don't know what to do about it, so we'll just Google it together."* (P11, Case manager)

Of course the quality of information gleaned from general web searches may be suspect, particularly when general privacy information is not well-suited to IPV situations. Examples of the latter include privacy suggestions directed at the public that do not account for IPV safety issues such as escalation (discussed in detail below). A number of professionals did turn to online resources that specifically target IPV contexts. Several mentioned making use of the websites and guides curated by the NNEDV[3] and Safe Horizons[4]. These organizations provide a number of useful documents, including high-level summaries of how to think about digital privacy and safety, guides about

[3] http://nnedv.org/resources/safetynetdocs.html
[4] https://www.safehorizon.org/wp-content/uploads/2016/06/1412609869_Tech-Safety-for-Victims-of-Abuse_Safe-Horizon.pdf

privacy settings for Facebook, and discussion of security practices such as picking strong passwords. They also discuss issues such as escalation and safety planning. As one attorney described,

> *"I get most of my safety tip sheets from the NNEDV, the Safety Net Project. So if they have something that's helpful, great, I can print it out and give it to a client. But if they don't, then we're kind of trying to figure it out, and so I'm like Googling stuff."* (P14, Staff Attorney)

However, as suggested in the quote, these documents do not cover all client technology issues. Guides typically only exist for popular, well-established websites and apps. For anything else, professionals must seek out their own information and interpret whatever they find in light of the threat model that their client is currently facing — a complex task even for technology experts. Even when documents relate to the technology at hand, they may be out of date (e.g., Facebook's default privacy settings have changed significantly over the years), or lack the detailed information needed to advise clients.

In addition to *"Googling-as-they-go"*, professionals said that they often turn to their peers for assistance with technology issues in the hope that the peer has experience with a particular technology or has previously had clients that faced similar technology problems. Such interactions represent one informal avenue by which ongoing professional training occurs in the IPV ecosystem. As a case manager told us,

> *"Usually I ask other people because chances are something may have happened to another client that is happening to my client, but I really wish that there was a more streamlined way of understanding this stuff because I really don't get it."* (P11, Case manager)

5.3.2 IPV professionals want technology training and new tools. The majority (n=32) of the professionals that we interviewed expressed a desire for more, and better, technology-focused training. When asked what would help them to deal with tech-enabled abuse, a case manager said,

> *"The technical? I think having trainings on how to get clients more tools, because we basically go by our own small knowledge of whatever we think. But not really of how clients should handle the stalking on, let's say Instagram or Facebook or things like that, and deactivating the page. Those kind of things will be helpful for our clients as well. How can they be more safe with technology and the abuser."* (P32, Case manager)

During our interviews, we heard about only a handful of sporadic training events provided by police officers from the NYPD, although the OCDV and partner organizations have recognized the need for more training programs, and one new program was started while our study was ongoing. Attorneys from Day One[5] held a seminar to train advocates to, in turn, train other professionals on digital privacy and safety topics. The training series primarily focused on raising awareness of tech-born threats (e.g., cyberstalking, revenge porn, spoofing), tech safety planning, and curriculum development for future trainings. Although several participants were able to attend the training and appreciated the information, they found the information to be relatively high-level, such as describing what spoofing is, rather than advising specific actions for advocates to take when their clients encounter spoofing.

5.4 Technology advice and assistance given to clients

Having developed an understanding of professionals' existing knowledge and strategies for finding tech-related information, we now discuss the advice and assistance that they offer clients.

[5] An organization working to end dating abuse and domestic violence, specifically focused on young people (https://www.dayoneny.org/).

Unsurprisingly, many professionals perceived their ability to give good technology advice to be hamstrung by their limited expertise and resources. One case manager told us,

> *"Our basic things are changing numbers, turning off GPS, things like that. But after that, I feel we don't know what to do … when it comes to tech, I don't think we know enough to be able to stop it."* (P11, Case manager)

Common *"basic things"* consisted of advice related to both software and hardware. Software advice that we heard frequently included: changing passwords and password recovery questions, limiting or restricting the sharing of pictures, blocking other users on social media, changing privacy settings (e.g., for Facebook), and deleting or shutting down online accounts. Common hardware advice included: throwing away the device, changing the SIM card or wireless plan, inspecting the device for unwanted apps (often by taking it to an official company store like the Apple store), performing a factory reset on the device, and turning off services like location and WiFi. Despite all this, victims and professionals identified a number of challenges that often prevent delivery of *useful* technology advice and assistance, as we now discuss.

5.4.1 Actionable versus general advice. One common challenge that we observed was a lack of *actionable* advice, defined as advice that equips a victim with sufficient knowledge to execute changes in the configuration or use of their device. There are two aspects to the sufficiency of knowledge required for actionable advice: (1) it readily suggests a course of action to the recipient, and (2) it contains sufficient detail to allow the recipient to execute that course of action. For example, an actionable piece of advice would be specific instructions on how to turn off location tracking on an Android phone. By contrast, general advice would be that victims should review their phone's location settings.

Several of the professionals that we interviewed expressed frustration that although they understood and could give clients general advice, they did not feel equipped to provide actionable advice. One case manager said,

> *"Sometimes, depending on the device, I won't really know how to help them. So like one time, it was an iPhone and I didn't have an iPhone. I only used Android, but I reached out to someone who did and kind of helped guide them, but in those cases if I don't really know, I'd just refer them back to the company, the provider."* (P30, Case manager)

Most online resources and training materials likewise consist of general advice. On one hand, the velocity of technology change means that actionable advice becomes stale quickly, whereas generalized advice enjoys more longevity. On the other, the efficacy of general advice relies on a victim being able to concretize it for their particular circumstances. However, as discussed in previous sections, many victims have insufficient technology know-how to do so. One client said,

> *"With all these apps, some of them I don't understand. When you get an app and it asks your permission, it says allow or deny. Allow this app to access your device or information, what does it mean? I would say no. Because I'm serious, I don't trust them. Because it seems – I heard the stories like anybody can log into your device, find out information. These apps ask this permission. What is that for?"* (P25, Client)

This quote surfaces another issue with (actionable) advice: the extent to which victims understand the likely ramifications of following it. On the technical level, this means understanding how the behavior of technology will change if the advice is followed. On the contextual level, this means being able to envision how those technical changes will modify the victim's situation. Both aspects of understandability are key for making informed decisions about whether to follow advice.

5.4.2 Lack of best practices for assessing technology risks. The wide variety of organizations involved in the IPV ecosystem means that different professionals utilize different protocols when performing intake, assessment, and safety planning[6]. One thing in common across organizations was the lack of formal materials or procedures that covered technology. Only four professionals mentioned that their approach to safety planning with clients routinely includes discussion of digital risk factors (e.g., use of Facebook, abuser access to devices). Thus, the most common situation that emerges from our interviews is one in which it is up to the client to offer details about any real or perceived technology issues. Most professionals (n=27) reported that technology only came up in their interactions if clients brought it up. One case manager described,

> *"The client will bring it up. I don't think I necessarily ask for it. Unless they give me a hint, but yeah, it's usually the client. Spyware, they don't really tell me an app name. They just tell me that they think their phone has some sort of spyware."* (P30, Case manager)

Leaving the client to bring up technology issues is driven in part by the fact that many interviews by professionals are *purposefully* client-driven. Rather than peppering the client with a standard set of questions, which may make them feel interrogated, professionals instead ask what brought the client in and let the conversation go from there. Although this approach may work well for issues such as physical abuse, that are widely recognized and whose symptoms are appreciated, the lack of best practices combined with the general lack of technology expertise described by both clients and professionals could be problematic: clients may not realize that technology is playing a role in their abuse, fail to bring it up in their meeting with the professional, and, if the professional never asks, the abuse could remain undetected and unaddressed.

5.4.3 Disconnecting is not always a good option. One frequent piece of advice given to clients is to entirely disconnect from one or more technologies: delete Facebook, throw away devices, turn off all location services, remove cameras or baby monitors from the home, etc. This approach clearly favors security and privacy and is, in the estimate of professionals, most likely to eliminate technology-related threats. As one social worker said,

> *"Delete your Facebook completely. Delete everything so he doesn't have access to you this way. Just throw away your phone and get a new phone."* (P18, Social worker)

In the most dangerous situations, such a scorched-earth approach to technology security and privacy may be appropriate. However, for many clients such an approach is impossible. In cases where the client and abuser share children, and the abuser has visitation rights, the client and abuser are required by law to have some means of communicating to coordinate childcare and visits. Several professionals also pointed out that disconnecting can often be detrimental for clients for a number of reasons. Most obviously, it cuts clients off from their professional and social support networks. Many clients are immigrants, and technology is often the only mechanism that they have to communicate with family and friends in their home country — a crucial source of social support. Given that a frequent abuser control tactic is to isolate victims from their networks, disconnecting can feel to clients like a continuation of the control exerted over their lives by the abuser. Another safety concern is escalation. Many professionals noted that it was sometimes not safe to cut off communication entirely, as the resulting loss of control for abusers can lead to increased physical safety risks. One case worker told us,

> *"[Disconnecting] often makes it worse. Clients are much more at risk when they actually separate from their abusers because he suddenly no longer has any control over that victim. So often the only thing left is through the phone, so he's going to start harassing you,*

[6] As discussed earlier, each FJC has a single intake form, and each resident organization has their own, often more detailed, intake form.

> *calling, texting. If you change your number, now he's most likely going to go crazy. So that's when he's going to start stalking you any way he can."* (P18, Social Worker)

Moreover, in managing an abuse situation, professionals and clients described how it was sometimes possible to use communications from an abuser to keep an eye on the situation and maybe provide advanced warning about threatening actions (e.g., physical attacks). In these situations, technology can provide clients with better control over the communication with their abuser. As one case manager described,

> *"Normally what the client does is block the person. But once they're blocked, they really don't know what's happening in the abuser's mindset. So they feel like he's going to show up. We say, "Okay, so what are some other ways he could contact you?" Well, we could do Facebook messages or WhatsApp . . . So that's the way they know how the abuser thinks or what might work. And at that point, if it's a stalker or someone that just wants communication, they'll take whatever you give them. They just don't want to get cut off."* (P32, Case manager)

5.4.4 The clients are in charge and make their own decisions. Most professionals emphasized that they try to avoid telling clients what to do, and instead view their job as simply providing clients with information and options. The clients should be the ones deciding, for example, what technology advice to ignore and what to follow. As one attorney told us,

> *"One of the tenets we have when we work with survivors is we let them have their own autonomy. Because they have been in such a controlling relationship that the last thing we want to do is tell them how to live their life. So we never tell them what to do. We always defer to them and assume that they have the best judgment about what's safe and what's not safe."* (P29, Staff Attorney)

However, deciding the best course of action when it comes to technology often requires clients to negotiate several tricky tensions. These include the ones discussed, such as clients wanting to cut off contact versus maintaining their social network or avoiding escalation. Another tension is between legal procedures and avoiding technological abuse, as discussed in the next section. Deciding the best course of action in the face of these trade-offs is often stressful, particularly when clients feel that they lack sufficient knowledge to fully understand the risks and repercussions.

5.5 Technology, the Law, and Legal Procedures

Legal procedures play a crucial role in protecting clients by helping to prosecute offenders and/or secure legal orders of protection that prevent abusers from seeing or contacting clients. We now discuss how technology intersects with the law.

5.5.1 Legal systems lack technology expertise. Many stakeholders in the legal system lack technology expertise. In addition to the attorneys' self-described lack of knowledge (discussed in previous sections), participants described how judges often lack the knowledge required to understand how technology is being used in IPV. An attorney said,

> *"Some [judges] are not familiar with Facebook, right? Or they vaguely know Facebook but don't understand how it works. Trying to explain to that judge about tech . . . it went right over the judge's head. She had no idea what I was talking about."* (P14, Staff Attorney)

Several participants described how technology plays an important role in gathering digital evidence, since most images, text messages, or social media posts are automatically saved and timestamped. We discovered that the current state-of-the-art for presenting digital evidence is for clients to capture screenshots of relevant content that are then printed out on paper and taken to

court, often with the goal of convincing a judge to issue an order of protection. In cases where there has been long-term abuse, this often amounts to *"hundreds and hundreds"* of printouts. Capturing evidence is further complicated by the rapid pace of technology change, since legal professionals need to learn about each new app or platform and develop procedures for collecting evidence. An attorney told us,

> *"I didn't know what WhatsApp was until a client came in and said, "Oh, he's been texting me and texting me." I'm like, okay, let's look through your texts. There wasn't anything in her texts, and I'm like, "What do you mean?" She's like, "No, no, he's been texting me on WhatsApp." I have no idea what that is. I had to start from scratch. What is this? What are the procedures?"* (P28, Attorney)

One ramification of the lack of technology expertise within legal systems is that there is currently little legal recourse for many forms of technology-enabled abuse. Participants described how technology was a good tool for abusers to be able to harass and stalk clients without much repercussion because, legally, there is not much that can happen to them. Many clients expressed frustration that police officers and attorneys would often listen to their stories but tell them *"there is nothing we can do"*. For example, a client who tried to apply for an order of protection based on Facebook abuse said,

> *"I feel the judge didn't really pay attention to the damage [the abuser] has done to me … he did not issue an order of protection that protected me from digital abuse. He just told [my abuser], "Oh, well, you should not post anything on Facebook about your wife" … but this has done so much damage to me emotionally."* (P23, Client)

Although this client blamed the judge for failing to act, her frustration is traceable to the lack of legal cognizability for many forms of technologically-mediated abuse. To try and overcome these challenges, some professionals described how they would work to tie the digital abuse to offenses that *are* recognized by the law. A police officer told us,

> *"You have to figure out how to tie it all together besides Facebook, because if you don't have an order of protection, he's not violating. So maybe we can tie it to stalking, which would be a misdemeanor. He can get arrested. She can get her order of protection."* (P27, Police Officer)

The subtlety here is that while an order of protection can be used to legally restrict abusers from contacting clients via Facebook, abusive messages on Facebook are not recognized as a form of abuse that warrants an order of protection.

5.5.2 The challenges of proving technology-enabled abuse. In addition to being constrained by what legally constitutes abuse, our findings also highlight that it is often challenging to collect digital evidence and prove technology-enabled abuse. For example, abusers frequently gain access to clients' devices and accounts, and several clients described how their abusers had deleted all of the digital evidence they had been saving to use in court (including photos of physical injuries). Without this evidence, there is often no way to prove abuse. In addition, there is confusion around the legal ownership of content created consensually (e.g., intimate photos or videos), but that the abuser then posts publicly without the client's consent.

To further complicate the process of proving digital abuse, abusers frequently set up anonymous email and social media accounts from which they harass the client, create fake Facebook pages containing harmful content, or use software to obscure their phone number when they send abusive text messages. In many cases, it can be extremely challenging or impossible to legally prove that it is the abuser who is behind the harassment, and the situation becomes even more complicated as the attacks become more technically sophisticated, such as email or text message spoofing.

Moreover, even when the abusive content is sent from the abuser's recognized phone number or online account, it can be difficult to hold them accountable because, as a social worker described,

> *"Most of the time, you have no evidence of who's posting it. Like a text message, right? He texted, "I'm going to kill you." Sometimes you will talk to an officer and they will tell you, "But how do we know it's him for sure?" . . . Technically anyone could have taken his phone and written that message. It's usually not regarded as strong evidence of abuse."* (P18, Social worker)

In working to preserve digital content for use in legal procedures, many professionals described that it could be challenging to communicate with Internet and social media companies. Although there were a few online platforms (e.g., Facebook and Instagram) that participants said were relatively good about responding to requests from law enforcement, many other companies were described as being either impossible to contact or simply ignoring requests. One attorney described their process for preserving an Instagram page,

> *"I was able to send a preservation letter to Instagram to preserve the page. Then I used information from the client to get a subpoena to find the IP address that he used to set it up. Once all that was done we told Instagram to take it down."* (P28, Attorney)

However, although useful for evidence collection, these legal procedures also result in a challenging trade-off for clients. On one hand, clients desperately want to permanently delete harmful or humiliating content. As an attorney described,

> *"I don't think a lot of our clients want to see the abusive and harassing things that people are sending them. It's easier to cope if it's not staring them in the face every day, so a lot of clients delete things because they don't want to look at it anymore."* (P25, Staff Attorney)

On the other hand, it is often necessary that clients preserve this abusive material if they want to obtain legal services and protection from the abuser. Managing this trade-off can result in distress and anxiety for clients who frequently feel that they are the ones being punished for somebody else's crime.

Finally, although, many social media platforms already provide mechanisms by which people can report abuse, many of our participants did not have the technical knowledge to find and use these reporting mechanisms. Moreover, when participants did try to report abuse, they told us that their requests often went unanswered. One client said,

> *"And even when you press something and say that you want to report this for offensiveness or abusiveness, they don't do anything about it."* (P2, Client)

One reason for this lack of action could be that much of the abuse that takes place in IPV settings may be too subtle for the platform in question to officially tag as abusive (e.g., comments that appear to be innocuous to an outsider that are threatening to a victim of IPV).

6 DISCUSSION

Having developed a nuanced understanding of the role that technology plays in the IPV ecosystem, we now synthesize our findings into recommendations for HCI and technology experts interested in aiding victims of abuse through design and technology. Our findings show that the IPV context provides a clear case where greater involvement by technologists is both needed and warranted. There are several entry points in the ecosystem of IPV services where technologists' expertise might make a marked difference in the effectiveness of service provision and positively impact the lives of IPV survivors.

First, our analysis clearly reveals a deep and urgent need for better information and training when it comes to technology and abuse — for both clients and professionals. In addition, although

there are a number of instruments to formally assess physical risk, such as the danger assessment for homicide risk [6], there are no such standard assessments for technology. Our findings highlight opportunities for future research to help develop digital risk assessment instruments, or augment existing instruments, to better account for the growing role of technology in IPV. Technologists could also work with legal professionals to develop new techniques for collecting legally valid digital evidence, including methods for holding abusers accountable by proving digital abuse.

However, technologists' entry into the IPV space must be sensitive to the unique needs and constraints of this ecosystem. Context-sensitive design is a watchword of effective technological intervention [1], but bears special weight in IPV. Without a deep understanding of the unique complexity of technology's role in the IPV ecosystem, technologists risk interventions that may be not only ineffective, but potentially *detrimental*, to stakeholders' physical, emotional, legal, and social needs. As Woelfer and Hendry [41] suggest, digital interventions create risks for vulnerable people, particularly around questions of visibility and detectability; they implore designers to act with abundant precaution in ensuring that the well-meaning systems they implement take full account of these risks. A key goal of our analysis is to illuminate these complexities in the interest of informing future interventions in the IPV context.

Many of the complexities that we discuss arise, in part, because victims do not *"escape"* from IPV in a discrete, complete way. They remain entangled with and tethered to abusers through familial and social connections; they try to maintain stable relationships for the sake of children; they are bound by legal agreements, emotional involvement, and economic necessity. Taking privacy-protective measures can, rather than decreasing abuse or affording victims more autonomy and freedom, serve to *escalate* abuse by frustrating the abuser. Digital abuse is situated alongside physical, emotional, psychological, and other forms of abuse; reducing an abuser's capacity to abuse through digital means may exacerbate abuse through other channels. Though it may seem counter-intuitive, maintaining open lines of digital communication with an abuser may actually make a victim safer by keeping the abuser physically at bay.

Privacy-protective measures can also conflict with the legal, social, and economic needs of victims. Establishing and preserving records of tech-enabled abuse can be crucial for obtaining protective orders, favorable custody agreements, and criminal convictions. However, such digital evidence is also a painful reminder of hurtful and/or humiliating experiences that a client would prefer to forget. Cutting off access to technology can degrade victims' access to social networks, hindering access to the strong social support that has been shown to help protect victims against the negative effects of IPV on mental and physical health [8, 9]. Similarly, technology is now necessary to navigate economic opportunities or maintain employment, as we saw in cases where social media was necessary for finding employment.

Our findings regarding these complexities corroborate and extend findings in recent work by Matthews et al. [26], which also highlights some of the tensions in mitigating technology-mediated IPV. Our work builds on theirs by painting a rich picture of the broad ecosystem that surrounds survivors of IPV; in so doing, we demonstrate that addressing these tensions requires careful attention to the needs, constraints, and roles of multiple stakeholders engaged in this complex ecosystem, not just those of the survivors. For example, developing and deploying new privacy-protection controls for social media, mobile devices, or other software may have little positive impact for survivors unless they take into account the level of technological expertise of both professionals and survivors. Engaging both clients and professionals in co-design of new controls, along with developing processes that make it easy for professionals to help clients navigate such controls, will be more likely to lead to successful interventions.

A similar viewpoint could be taken for creating new procedures for reporting, and retaining evidence of, online abuse. Our findings show that the victims of IPV are often not the ones who

work to get abusive content removed from social media platforms. Instead, it is typically legal professionals, working on behalf of their clients, who communicate with the software companies. Thus, there is scope for new streamlined reporting mechanisms that specifically target legal professionals and that make it easy for them to communicate with software companies about IPV-related content. Similarly, any new methods for collecting digital evidence should take into account the safety and privacy of victims, but also the needs of the legal professionals — attorneys and judges — who will evaluate the evidence in court.

Moreover, technologists interested in creating interventions that aid survivors of IPV must recognize that the technology cannot be developed in isolation. Instead, technical advances will need to be accompanied by parallel advances in legal and social support systems. For example, developing new techniques to collect legally valid digital evidence will require the legal system to evolve so as to recognize the new techniques. Similarly, developing new digital risk assessment instruments would require the professionals at the FJCs to change their procedures to incorporate these instruments into standard practice. Thus, it is essential that technologists work in concert with other stakeholders in the IPV ecosystem if they are to develop interventions that have a positive impact.

Finally, we acknowledge that our study took place within the context of the IPV ecosystem in NYC and we readily admit that some of our findings may be limited to the institutional specificities of this context. Although generalizability is not a goal of our study, we expect that many of the technology-related risks, tensions, challenges, and trade-offs that came up in our study will be relevant for IPV ecosystems in general, and we hope that our findings will be useful for HCI and technology experts interested in designing technologies to aid IPV survivors in a range of settings.

7 CONCLUSION

This paper presented a qualitative study that analyzed the role of digital technologies in the IPV ecosystem in NYC. We described a complex set of socio-technical issues that impact IPV settings and complicate digital privacy and safety for survivors of IPV. We highlighted stakeholders' varying levels of technology expertise and discussed a range of strategies used to provide survivors with advice and assistance. We also revealed a number of tensions and trade-offs in negotiating technology's role in social support and legal procedures. Taken together, our findings contribute a nuanced understanding of technology's role in IPV and suggest a number of recommendations for HCI and technology experts interested in aiding victims of abuse via design and technology.

8 ACKNOWLEDGMENTS

We would like to thank all of our partners and collaborators at the New York City Mayor's Office to Combat Domestic Violence and the Family Justice Centers. We would also like to thank all of our participants for their willingness to share their stories with us. This work was supported in part by NSF grant CNS-1330308 and a Sloan fellowship.

REFERENCES

[1] Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. 1999. Towards a better understanding of context and context-awareness. In *International Symposium on Handheld and Ubiquitous Computing*. Springer, 304–307.

[2] Carmen Alvarez, Gina Fedock, Karen Trister Grace, and Jacquelyn Campbell. 2016. Provider screening and counseling for intimate partner violence a systematic review of practices and influencing factors. *Trauma, Violence, & Abuse* (2016).

[3] 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 *Workshop on Privacy in the Electronic Society*. ACM, 201–204.

[4] 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.

[5] Michele C Black, Kathleen C Basile, Matthew J Breiding, Sharon G Smith, Mikel L Walters, Melissa T Merrick, Jieru Chen, and Mark R Stevens. 2011. The national intimate partner and sexual violence survey (NISVS): 2010 summary report. *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention* 25 (2011).

[6] Jacquelyn C. Campbell, Daniel W. Webster, and Nancy Glass. 2009. The Danger Assessment. *Journal of Interpersonal Violence* 24, 4 (2009), 653–674.

[7] 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.

[8] Ann L Coker, Paige H Smith, Martie P Thompson, Robert E McKeown, Lesa Bethea, and Keith E Davis. 2002. Social support protects against the negative effects of partner violence on mental health. *Journal of women's health & gender-based medicine* 11, 5 (2002), 465–476.

[9] Ann L Coker, Ken W Watkins, Paige H Smith, and Heather M Brandt. 2003. Social support reduces the impact of partner violence on health: application of structural equation models. *Preventive medicine* 37, 3 (2003), 259–267.

[10] 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 ACM International Conference on Ubiquitous computing*. ACM, 321–330.

[11] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5 (2011), 413–421.

[12] 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.

[13] Martin Emms, Budi Arief, and Aad van Moorsel. 2012. Electronic footprints in the sand: Technologies for assisting domestic violence survivors. In *Annual Privacy Forum*. Springer, 203–214.

[14] 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.

[15] Joel H Garner and Christopher D Maxwell. 2008. Coordinated community responses to intimate partner violence in the 20th and 21st centuries. *Criminology & Public Policy* 7, 4 (2008), 525–535.

[16] Reem M Ghandour, Jacquelyn C Campbell, and Jacqueline Lloyd. 2015. Screening and counseling for intimate partner violence: A vision for the future. *Journal of Women's Health* 24, 1 (2015), 57–61.

[17] Nancy Glass, Stephen Dearwater, and Jacquelyn Campbell. 2001. Intimate partner violence screening and intervention: data from eleven Pennsylvania and California community hospital emergency departments. *Journal of Emergency Nursing* 27, 2 (2001), 141–149.

[18] Maritza Johnson, Serge Egelman, and Steven M Bellovin. 2012. Facebook and privacy: it's complicated. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, Article 9, 9:1–9:15 pages.

[19] Carol E Jordan. 2004. Intimate Partner Violence and the Justice System An Examination of the Interface. *Journal of interpersonal violence* 19, 12 (2004), 1412–1434.

[20] 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 *Symposium on Usable Privacy and Security (SOUPS)*. 39–52.

[21] Andrew King-Ries. 2010. Teens, technology, and cyberstalking: The domestic violence wave of the future. *Tex. J. Women & L.* 20 (2010), 131.

[22] Etienne G Krug, James A Mercy, Linda L Dahlberg, and Anthony B Zwi. 2002. The world report on violence and health. *The lancet* 360, 9339 (2002), 1083–1088.

[23] Christopher A. Le Dantec, Robert G. Farrell, Jim E. Christensen, Mark Bailey, Jason B. Ellis, Wendy A. Kellogg, and W. Keith Edwards. 2011. Publics in Practice: Ubiquitous Computing at a Shelter for Homeless Mothers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. 1687–1696.

[24] Karen EC Levy. 2014. Intimate surveillance. *Idaho L. Rev.* 51 (2014), 679.

[25] Michael Massimi, Jill P Dimond, and Christopher A Le Dantec. 2012. Finding a new normal: the role of technology in life disruptions. In *ACM Conference on Computer Supported Cooperative Work*. ACM, 719–728.

[26] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy and security practices when coping with intimate partner abuse. *ACM Conference on Human Factors in Computing Systems* (2017), 2189–2201.

[27] Virginia A Moyer. 2013. Screening for intimate partner violence and abuse of elderly and vulnerable adults: US preventive services task force recommendation statement. *Annals of internal medicine* 158, 6 (2013), 478–486.

[28] Christine E Murray, G Evette Horton, Catherine Higgins Johnson, Lori Notestine, Bethany Garr, Allison Marsh Pow, Paulina Flasch, and Elizabeth Doom. 2015. Domestic violence service providers' perceptions of safety planning: a focus group study. *Journal of Family Violence* 30, 3 (2015), 381–392.
[29] Shirley Patton. 2003. Pathways: How women leave violent men. *Partnerships Against Domestic Violence* Vol. 1 (2003).
[30] 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.
[31] 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.
[32] Safe Chat Silicon Valley. 2017. Safe Chat Silicon Valley. (2017). http://safechatsv.com/.
[33] 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.
[34] David R Thomas. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation* 27, 2 (2006), 237–246.
[35] National Network to End Domestic Violence. 2017. Tech Safety App. (2017). https://techsafetyapp.org/.
[36] Kylee Trevillion, Bryony Hughes, Gene Feder, Rohan Borschmann, Siân Oram, and Louise M Howard. 2014. Disclosure of domestic violence in mental health settings: A qualitative meta-synthesis. *International Review of Psychiatry* 26, 4 (2014), 430–444.
[37] National Coalition Against Domestic Violence. 2017. Statistics. (2017). http://ncadv.org/learn-more/statistics.
[38] Jill Waalen, Mary M Goodwin, Alison M Spitz, Ruth Petersen, and Linda E Saltzman. 2000. Screening for intimate partner violence by health care providers: barriers and interventions. *American journal of preventive medicine* 19, 4 (2000), 230–237.
[39] Lenore E Walker. 1977. Battered women and learned helplessness. *Victimology* (1977).
[40] Rick Wash. 2010. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, Article 11, 11:1–11:16 pages.
[41] Jill Palzkill Woelfer and David G Hendry. 2011. Designing ubiquitous information systems for a community of homeless young people: precaution and a way forward. *Personal and Ubiquitous Computing* 15, 6 (2011), 565–573.
[42] Delanie Woodlock. 2016. The abuse of technology in domestic violence and stalking. *Violence against women* (2016).
[43] Min Xie, Janet L Lauritsen, and Karen Heimer. 2012. Intimate partner violence in US Metropolitan areas: The contextual influences of police and social services. *Criminology* 50, 4 (2012), 961–992.