"Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence

DIANA FREED*, Information Science, Cornell Tech, USA
SAM HAVRON*, Computer Science, Cornell Tech, USA
EMILY TSENG, Information Science, Cornell Tech, USA
ANDREA GALLARDO, Information Science, Cornell Tech, USA
RAHUL CHATTERJEE, Computer Science, Cornell Tech, USA
THOMAS RISTENPART, Computer Science, Cornell Tech, USA
NICOLA DELL, Information Science, the Jacobs Institute, Cornell Tech, USA

Intimate partner abusers use technology to track, monitor, harass, and otherwise harm their victims, and prior work reports that victims have few resources for obtaining help with such attacks. This paper presents a qualitative analysis of data from a field study of an approach to helping survivors of intimate partner violence (IPV) with technology abuse. In this approach, called clinical computer security, a trained technologist performs a face-to-face consultation with an IPV survivor to help them understand and navigate technology issues. Findings from consultations with 31 survivors, as well as IPV professionals working on their behalf, uncovered a range of digital security and privacy vulnerabilities exacerbated by the nuanced social context of such abuse. In this paper we explore survivor experiences with, and reactions to, the consultations, discussing (1) the ways in which survivors present their tech concerns, (2) the cooperative work required to guide survivors towards understanding probable causes of tech insecurity, (3) survivors' reactions to the consultations, particularly when security vulnerabilities or spyware are discovered, and (4) the role we play as consultants and interventionists in the complex socio-technical systems involved in mitigating IPV. We conclude by discussing some of the broad ethical and sustainability challenges raised by our work, and provide design opportunities for tech platforms to better support survivors of IPV.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**;

Additional Key Words and Phrases: Intimate partner violence, gender-based violence, privacy, security

ACM Reference format:
Diana Freed*, Sam Havron*, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. *"Is my phone hacked?"* Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 202 (November 2019), 24 pages.
https://doi.org/10.1145/3359304

1 INTRODUCTION

Intimate Partner Violence (IPV) is a widespread global problem, affecting one out of three women and one out of six men over the course of their lives [56]. Defined as violence enacted against

*These authors contributed equally to the paper.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2019 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.
2573-0142/2019/11-ART202 $15.00
https://doi.org/10.1145/3359304

an individual by an intimate partner, typically a current or former significant other, IPV presents unique challenges for digital privacy and security. Indeed, a number of recent studies have painted an increasingly detailed picture of the ways in which abusers use technology to harass, monitor, and harm their intimate partners [10, 17, 32, 33, 48, 57, 68]. However, although this body of prior work extensively documents the complex tech abuse challenges that IPV victims and professionals face, few studies, if any, describe interventions or constructive approaches toward directly improving people's lives. Meanwhile, the professionals currently helping victims, for example social workers and lawyers, acknowledge they have insufficient understanding of technology to properly assist [32].

A recent paper [37] describes an intervention we have been exploring called "clinical computer security". The idea is for trained technologists to provide face-to-face consultations with victims to help them navigate possible tech abuse, supported by a set of custom tools that help surface vulnerabilities. The consultation protocol is structured around a referral model in which an IPV professional refers a victim—called a client in this context—for assistance with tech issues. One or more tech consultants meet with the client face-to-face and follow a procedure built around (1) understanding the client's concerns via discussion and questions that surface common problems, (2) investigating the client's technology via manual inspection of devices and accounts and programmatic scans of devices for spyware or other dangerous apps, and (3) advising the client and IPV professional about how to potentially mitigate discovered issues. Importantly, this last part feeds into a safety planning process ideally involving the client, IPV professional, and consultant.

Working with the New York City Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV), we performed a field study of the intervention with 31 clients at ENDGBV facilities called Family Justice Centers (FJCs).[1] In [37], we describe in detail the careful process we went through to design our consultation protocol and associated tools, and present some initial quantitative results from the field trial. Following that work, in this paper we offer a qualitative analysis of the audio-recorded consultations with IPV survivors that we collected during the field trial to contribute an understanding of: (1) the ways in which clients present their tech concerns, (2) the cooperative work required to guide clients towards understanding probable causes of tech insecurity, (3) clients' reactions to the consultations, particularly when security vulnerabilities or spyware are discovered, and (4) the role we play as consultants and interventionists in the socio-technical systems involved with mitigating IPV.

Perhaps unsurprisingly, given prior works' descriptions of survivor problems [32, 33, 48, 68], we found that clients often present their concerns in a technologically ambiguous way (e.g., voicing concerns about being "hacked"). Such ambiguity, together with the intricacy of clients' digital footprints—the sets of interconnected devices, accounts, and other technologies with which clients interact—can pose a significant challenge to understanding their concerns and vulnerabilities. This challenge is further complicated by social entanglements that further enable tech abuse.

The technical instruments used in our consultations also played an important role in discovering probable explanations for clients' reported tech issues. As detailed in [37], this required working with clients to log into their accounts and devices, before manually and programmatically inspecting them for indicators of compromise. We found that clients readily trusted us with their devices and, more broadly, that both clients and professionals immediately treated consultants as experts on tech issues. This in turn raised challenges when clients expected consultants to also provide advice on non-technical issues, for example, best practices for documenting forensic digital evidence for use in legal cases.

We conclude by reflecting on the broader issues raised by our work. We discuss how, by intervening in the complex, socio-technical systems found in IPV contexts, we also change the realities

[1] All protocols were approved by our institutional IRB and ENDGBV leadership.

of these systems themselves [45, 53, 59]. For example, our intervention changes the ecosystem of support services available to IPV victims, leading to a new dependence on us for tech assistance. This dependence in turn raises ethical questions about how to sustain, and possibly scale, our clinical security interventions. Lastly, we discuss suggestions for how technologies may be better designed to aid IPV victims, tech consultants, and technology users in general.

2 RELATED WORK

Recent threads of work in HCI generally and CSCW specifically have sought to establish theoretical foundations for technology design projects aimed at improving the lives of oppressed or targeted people. Ranging from domain-specific frameworks for health equity [58] to HCI4D [15, 44] to broad examinations of technology's potential in social justice [19, 30] or design justice [13, 25], these works share a common concern: thoughtful examination of the role technologists play as interventionists in these contexts. Bardzell [5] described such technology design as an aspiration towards technologists as advocates and outlined its essential tension as a dilemma between perpetuating oppressive status quos in the name of usability and imposing the technologist's own values on others.

Against this landscape, our work centers on a particular type of intervention: sociotechnical systems supporting *consultation*, where an individual facing a specific problem (the client) seeks help from another individual or organization (the consultant) dedicated to providing specific forms of assistance. CSCW has contributed significantly to the development of such systems in medical environments, where the interactions between patients and healthcare providers are increasingly inextricable from electronic health records [28, 50]. While previous threads of work have focused on the consultant as a facilitator of the client's own work towards their goals [63], recent research has framed the consultation as a site of collaborative epistemic generation, in which the consultant participates in sensemaking through the act of recording the client's narrative [4]. We extend these lines of inquiry with a case study of how the technologist-as-consultant dynamic plays out in a new context: a socio-technical system built to aid victims of technology-mediated IPV.

2.1 Technology-enabled IPV

A growing body of research documents how abusers exploit technology to harm their intimate partners [10, 17, 32, 33, 47, 48, 57, 68]. Freed et al. [33] demonstrate the complexity of tech-based attacks that IPV victims experience, categorizing these attacks into: (1) ownership-based attacks in which the abuser owns the victim's accounts or devices, giving them access and control, (2) account or device compromise, such as guessing or compelling disclosure of passwords, (3) harmful messages or posts (e.g., on social media), and (4) exposure of private information. Much of this work discusses how tech abuse in IPV involves complex socio-technical and relational factors due to the intimacy of the relationship, largely differentiating this context from other forms of abuse enacted through digital technologies, such as online harassment [36, 64, 66], doxxing [8, 20], cyberbullying [3, 18], and cyberstalking [22, 26, 31, 69]. Compounding these issues, research has also suggested that tech abuse in IPV can lead to physical confrontations or even murder [57].

This body of prior work also suggests that IPV victims currently have few effective options for obtaining assistance with tech abuse [32, 48]. First, victims' existing support structures often struggle in the face of the unique challenges presented by technology-enabled IPV. Although IPV professionals, like social workers, case managers and lawyers, increasingly find themselves assisting clients experiencing complex technology-enabled IPV, they uniformly report having insufficient computer security knowledge to effectively provide aid [32]. Some IPV support organizations provide trainings for professionals about tech risks, with a focus on raising awareness of general classes of threats such as spyware, spoofing, or doxxing, but these trainings usually do not include standardized procedures for flagging and addressing tech issues [32]. Similarly, the National Network

to End Domestic Violence (NNEDV) [61] and other organizations provide resources for professionals and victims, including advice guides and best practices, but prior work suggests that clients may struggle to use these guides on their own [32].

In complex cases, IPV professionals sometimes refer victims to general tech support services, such as cellular stores or GeekSquad. However, such services are frequently outside the socioeconomic means of IPV victims and, even when usable, may not be prepared to safely handle IPV tech abuse situations. Indeed, prior qualitative work with victims and professionals suggests that these services currently do not play a signi cant role in helping victims [32, 48].

Meanwhile, the privacy and security tools currently available for victims' use often have usability challenges that are exacerbated by IPV contexts, where victims are frequently facing persistent, targeted digital attacks [12, 41, 42, 65]. Arief et al. [2] seek to address this challenge via a vision of sensible privacy that takes into account IPV victims' particular requirements, and suggest an app that would help a victim erase information on their device related to visits to IPV-relevant websites. Emms et al. [23] similarly suggested tools for helping people erase browser histories. Other tools for survivors include the NNEDV's TechSafety app [62] and the Safe Chat Silicon Valley app [54], tools that provide victims with resources like safety planning [49]. Finally, collaborative online tools exist to help users defend against more general online harassment, but these tools often do not take into account the speci c threats facing IPV victims [7, 16, 38, 46]. Our work di ers from these approaches in that, instead of building a speci c app or tool for survivors, we work to deliver face-to-face, personalized consultations in which we help survivors of IPV analyze their technological assets and improve their ability to resist attacks. We now discuss our approach.

2.2 Clinical computer security interventions

In recent work [37], we have been developing a new approach to helping victims called clinical computer security. The idea is to have a trained technologist (consultant) collaboratively work with a survivor (client) and the IPV professionals helping them to navigate tech abuse. This idea, rst detailed in [37], is similar to e orts by the Citizen Lab [14] and Citizen Clinic [11] to help victims of digital attacks by nation-states, or the help provided by computer security experts on an ad hoc basis to individuals su ering harassment [39]. Similarly, a recent technology-enabled coercive control (TECC) clinic was established for IPV victims in Seattle [60]. However, our work is the rst research study to focus on the design of personalized interventions for tech abuse.

Our complementary paper [37] describes in detail the design of our clinical procedure, including how we arrived at the set of technical and non-technical tools that we use to understand clients' situations, investigate possible tech vulnerabilities, and advise them about potential next steps. That paper also provides a *quantitative* report on the eld study data from the researchers' perspective.

In contrast, this paper reports a detailed analysis of the *qualitative* data collected during the eld study, drawing primarily on transcripts of audio-recorded consultations and handwritten notes collected during our interactions with clients. We seek to answer important questions about the role of such interventions by making sense of the clients' experiences with, and reactions to, our consultations. We also re ect on our own role as interventionists in this complex socio-technical landscape, and the broader impact our interventions have on the survivor support community.

Consultation design. The design of our consultation protocols and instruments followed a careful, stakeholder-guided and iterative process (detailed in [37]). While the design of our consultations is not a contribution of this paper, we feel it is important to provide a brief overview of our consultation model since it provides essential context for understanding how we interacted with clients.

As discussed, our consultation procedure works within a referral model and follows a three-part framework: understand-investigate-advise. First, a client is referred to us by an IPV professional (e.g.

a social worker, lawyer, or case manager). Having an IPV professional involved enhances the safety of our interventions, and our protocol includes a safety planning discussion between the client and referring professional about the results of our technology consultation. This helps to avoid hasty decisions that may lead to issues such as escalation of the abuse (e.g., physical abuse in response to removing the abuser's access to the victim's digital assets).

Once a client is referred, we meet with them for a face-to-face consultation. These sessions begin with an open-ended discussion of the clients' concerns, the goal being for the consultant(s) to understand the client's situation. To help guide this discussion, we developed a technology assessment questionnaire, or TAQ (provided in Appendix A), that aims to uncover common vulnerabilities that have been identified in prior work [33]. We also try to map out each client's digital footprint their set of devices and accounts as well as their entanglements digital or social relationships that may enable or complicate tech abuse. To facilitate this mapping, we created a tool called a technograph (see Appendix B), that the consultant uses to draw relationships between people (e.g., client, abuser, children), devices, and accounts.

Once a consultant has a better understanding of the clients' situation, they investigate the client's technologies (devices and accounts), both manually and via programmatic tools. We designed account security checklists (see Appendix C) that guide the consultant through inspecting the client's accounts, including checks for spurious logins (e.g., unknown devices accessing their Gmail or Facebook accounts), whether location sharing is being used in Google Maps, security and privacy settings on Apple and Google apps, and more. We also built a tool called ISDi (Spyware Discovery) that uses a USB connection to an iOS or Android device to scan the set of apps installed and flag any that are potential spyware.

Finally, the consultant advises the client and referring IPV professional about what was discovered in the consultation, and describes any mitigations that might help the client. Importantly, our consultation procedure adopts a client-centered approach [34, 35, 52]. Considered a best practice in IPV advocacy more broadly, this mindset means that consultants assume the client is the ultimate authority on their situation. Consultants avoid being prescriptive (you should change your password) and instead try to be informative (you could change your password, which should prevent someone from being able to access your account). They also respect clients' choices about how to proceed (e.g., whether to ultimately change the password).

3 METHODS

The main goal of this paper is to understand IPV survivors' experiences with and reactions to our consultations. To achieve this goal, we conducted a qualitative analysis of data collected during 33 tech consultations with 31 IPV survivors that explores the following research questions:

(1) How do clients present their tech concerns, and what are the challenges involved in mapping these concerns to their digital footprints and entanglements?
(2) What is the work required to guide clients towards understanding probable causes of tech insecurity, and how do our consultations standardize the discovery of such causes?
(3) What are clients' reactions to our consultations, particularly when security vulnerabilities or spyware are discovered?
(4) What role do we play as consultants and interventionists in complex tech abuse situations?

Our study took place in partnership with the New York City (NYC) Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV) [24], which runs Family Justice Centers (FJCs) [29] that offer services for IPV survivors. All methods were approved by our university's IRB and the ENDGBV.

Recruitment. We distributed flyers at FJCs that made clients and professionals aware of the opportunity to participate in the study, advertising it as a tech safety and privacy consultation. The

ier directed clients to speak with their case manager who, after consulting with the client, booked an appointment for a day when we would be at the FJC. As FJC employees became aware of our work, they also began reaching out to schedule client appointments outside of our given dates.

Procedures. Consultations took place in a private room at every FJC. Each consultation was done by a team of two or three researchers: one person focused on communication with the client, another on the technical parts of the consultation (device scans, account security checks), and a third to take notes. We began by introducing ourselves and explaining the goals of the study. We also gave clients a consent form stating what we would do in the consultation. In accordance with our IRB, we did not ask clients to sign the consent form, to maintain anonymity.

We then proceeded with the consultation, as described in Section 2.2. We began with an open-ended discussion with the client that sought to understand their situation, tech abuse history, and main concerns. Then, we conducted manual and programmatic investigations of any accounts or devices that the client brought to the consultation. Finally, we engaged the client in a conversation about the consultation ndings, including problem mitigation advice and answers to questions.

Consultations lasted between 30 minutes and two hours, and we interviewed a minimum of one and a maximum of four clients on a single day. In seven cases, the clients preferred to have an IPV professional present for the consultation. At the end of the consultation, we thanked the clients for their time and gave them $10 compensation. The ENDGBV suggested this amount as being appropriate to cover the cost of transportation to and from the FJCs.

Participants. We conducted a total of 33 consultations with 31 IPV survivors (30 female, 1 male), who were all FJC clients. Two clients received follow-up consultations (at their request) to scan additional devices. All participants were adults, and all but one no longer lived with their abuser. We did not collect detailed participant demographics for safety and anonymity reasons, but note that they came from a wide range of ages and socioeconomic, ethnic, and cultural backgrounds.

Clients brought a total of 77 devices to the consultations: 46 Android or iOS smartphones, 13 tablets, 12 laptops, and six other devices. The six other devices, for which we did not have a protocol for an account security check, included three Amazon Echos, a Nintendo gaming system, a Blackberry phone, and a ip phone. We performed a best-e ort inspection in each of these cases, except for the ip phone, for which the client had no concerns. We used our account security check protocols to inspect all 71 other devices, and scanned all but ve smartphones and tablets using our ISDi tool. Three devices could not be scanned by ISDi due to errors (xes were made for subsequent scans), one client had to leave before we could scan their device, and another did not wish to have their phone scanned.

Data collection and analysis. Our data consist of the detailed notes taken during all consultations, as well as professional transcriptions of audio recordings made during consultations with clients' permission. Among 33 consultations, 24 consented to audio recording.

To analyze our notes and transcripts, we used a bottom-up thematic approach [ ], beginning with a detailed reading of the data, during which we allowed initial codes to emerge. Examples of initial codes include *fear of tech*, *account lockout*, and *client reaction*. We then performed multiple passes over the data to re ne the codes. Our nal set of 93 codes were formalized in a codebook that was used to perform a detailed analysis of all transcripts and notes. Examples of codes include *entanglement*, *client action*, and *iCloud compromise*. Finally, we clustered related codes into high-level themes that represent our prominent ndings. Examples of themes include *client concerns*, *feelings and reactions*, and *vulnerabilities discovered*.

Safety, privacy, and ethics. IPV survivors are a vulnerable, at-risk population. We took great care to ensure their safety and privacy. We did not ask participants to sign a consent form, collected

very limited demographic information, and did not record any identifying details about clients. The audio recordings of consultations do not mention clients' names, locations, or other identifying information, and thus using an audio transcription service posed minimal privacy risks for clients. All communication with clients outside of the consultation took place through their referring IPV professional. At the FJCs, an IPV professional was available at all times, in case a client or researcher needed additional support or advice. In addition, since changing privacy settings or uninstalling apps could lead to potentially dangerous escalation of abuse, whenever possible, we encouraged clients to have a trusted IPV professional present to safety plan before making changes.

In this paper, we have carefully anonymized client quotes and stories by removing potentially identifying phrasing. We have also removed names of any esoteric tools or apps. All tools mentioned by name (e.g., iCloud, Gmail) are very common and do not pose a risk to client anonymity.

We also took steps to protect the safety and well-being of our research team. Although our names and a liations were written on study materials (e.g., the consent form), we asked clients to use rst names only, in case an app was transmitting audio to an abuser. Moreover, working with IPV survivors can be mentally and emotionally challenging. After consultations, we met regularly as a group to debrief and have open discussions, and FJC sta graciously agreed to speak with researchers to help process their experiences.

Finally, we want to warn readers that our ndings contain information related to physical, emotional, and other kinds of abuse that some readers may nd distressing. Nevertheless, we believe it is important to report this information to the research community in the hope that it motivates researchers to work on the challenges presented by IPV.

4 FINDINGS

We begin by describing the challenges of teasing apart clients' concerns and complex digital footprints, and mapping them to potential vulnerabilities. We then describe how we worked collaboratively with clients and IPV professionals to apply our protocol for discovering tech vulnerabilities, including how our di erent instruments fared in practice. We discuss how clients reacted to both our consultation procedures and to vulnerabilities surfaced. Finally, we analyze our evolving role as tech consultants in the IPV ecosystem.

4.1 Understanding and mapping tech abuse

We found that, in practice, it is often extremely challenging to obtain a clear understanding of clients' chief concerns and to map them to potential attack vectors for investigation. We describe these challenges below.

Challenges identifying chief concerns. Core to our consultation is the identi cation of a client's chief concerns. Adapted from best practices in medicine (cf. [55]), where it is called the chief or presenting complaint, this step serves to focus the consultation on issues the client nds most pressing, rather than issues the consultant might think are important.

We enact this by beginning each consult with a conversation with the client, asking what has brought them to the consultation today. In response, clients used a wide range of language to articulate the concerns that brought them in. Fully 15 of our 31 clients reported generally suspicious behaviors from their devices, such as hearing static , crackles, beeps or echoes when using their device for phone calls. This led to concerns that their phones were being monitored; as one client said, I just want to know if my phone is being bugged (F4). In fact, general concerns of surveillance or monitoring by abusers surfaced in 18 of our 31 cases.

Seven clients reported that their abusers had hacked their accounts or devices, from email accounts and social media pro les to phones and laptops. The tech-savviness of abusers relative to

clients emerged as a key concern in our data: 11 clients reported abusers who had some background or interest in technology and/or the means to obtain IT expertise. These concerns were often accompanied by reports that abusers had access to information they should not otherwise have, such as the client's location, pictures, or browser history. As one client said,

> I told you, my phone is hacked. Maybe he has like ... a lot of information, because he's a person who spends money doing all these evil things. That's the person he is, and he can hire some IT person, and he can do it. That's how things are happening with me. (P27)

We encountered examples of chief concerns falling into all categories of the attack taxonomy described in Freed et al. [38]. We also uncovered many cases in which clients reported not just one chief concern, but rather a pattern of multiple concerns, e.g., digital monitoring as well as harassing text messages sent via spoofed phone numbers. This kind of multimodal abuse was reported by 19 of our 31 clients. As one described,

> He's tracking [everything]. Whatever I do, he sees that. Yesterday, I was [browsing the web], and he started to text me. He's harassing me until now. And then, because I have an order of protection, now he's using these spoo ng apps to harass me from di erent numbers. Although the police don't want to le a report because they're like, `You can't prove that that's him.' (P13)

Mapping concerns to clients' digital footprints and entanglements. Once we had identi ed clients' chief concerns, we faced the di culty of quickly understanding their socio-technical ecosystems and narrowing in on issues we should investigate for vulnerabilities. In this, our foremost challenge was understanding clients' digital footprints and potential entanglements.

We grappled rst with clients' digital footprints the set of devices and accounts the client owned or interacted with. The median number of devices a client brought was two, but we had clients that brought up to seven devices. Many clients had a large number of online accounts across email, banking, and social media; in most cases, a subset of these digital assets were reported to previously have been shared with, or compromised by, the abuser.

As one example of digital footprint complexity, we encountered four clients who took part in a shared family plan with their abuser or abuser's family members, even though they had physically left the relationship and the abuser no longer had direct access to their devices. One participant said she did not remember her login credentials to her cellular service account, and that she shared a plan with a close relative of the abuser: `Many years we've had the same account.' (P4).

The above is also an example of what we call entanglements: digital or social relationships that may complicate or enable abuse. In this case, the family member of the abuser provided an indirect route through which the abuser could monitor the client's digital activities. In 12 of our 31 cases, clients reported that abusers used these indirect routes to harass or intimidate them via proxies like children, coworkers, friends and random strangers.

To build a workable mental model of a client's digital footprint and entanglements, the consultant uses an instrument called the technograph (described in [37] and shown in Appendix B) to draw connections between people, devices, and accounts. Once we identi ed clients' chief concerns and made mappings to plausible technology abuse vectors (e.g., account compromise, spyware, family sharing, etc.), we faced the challenge of investigating the client's devices and accounts to discover evidence of vulnerabilities. Doing so required a standardized process, as we now discuss.

4.2 Standardizing the discovery of tech vulnerabilities

To surface potential security vulnerabilities in the client's digital footprint, we weave together semi-structured questions pulled from an instrument that we designed, called the TAQ, along

with manual investigations of client accounts and devices, and a programmatic scan of their devices for potentially dangerous apps. At a high level, our consultations surfaced important security vulnerabilities for 14 of the 31 clients in our study. As discussed below, these included possible password compromise, shared wireless family plans, the presence of potential spyware, and more. It is important to note that, in most cases, we do not have de nitive proof that abusers are actively exploiting these vulnerabilities, or that they are in fact the root causes of clients' problems. Nevertheless, given the high-risk nature of many IPV situations, all of the vulnerabilities we detected represent serious threats to client safety and security.

The TAQ. We designed a technology assessment questionnaire, or TAQ (provided in Appendix A), to help uncover vulnerabilities frequently encountered in IPV. For example, we ask how a client chooses their passwords and whether the abuser may know (or be able to guess) them. Prior work indicated this is a frequent vulnerability [32, 33, 48]. In response to this question, a client said,

> My password? It's [a family member's name] . . . and the number that I always use, that he knows that I use for everything. I know it's not a smart password. And the PINs for both devices are [a family member's] birthday. (P20)

This single question surfaced for eight clients that their passwords were either known or guessable by the abuser. And, as indicated above, some clients were aware of their insecure practices. The TAQ includes other questions about social media, family plans, child devices, and more. They proved a valuable reference for consultants, and at least some of them were used in every consultation.

Manual tech investigations. We found it valuable to manually investigate with clients various security and privacy settings that may help surface vulnerabilities. To facilitate this, we designed step-by-step guides for checking the security- and sharing-relevant settings of common platforms, including iCloud and other Apple services, Google, Facebook, Instagram, and more (see Appendix C). Particularly useful in our consultations were the security consoles that indicated what devices had recently accessed an account, as o ered by Google, Facebook, Instagram, iCloud, and Dropbox. None of our participants knew about this security feature beforehand.

Here, the bene ts of a face-to-face consultation were quite tangible. We sat side-by-side with the client, jointly inspected the list of recent devices accessing their account(s) and discussed with them whether they recognized the devices as their own or as associated with the abuser. Four clients' accounts were being accessed by devices that were either questionable or identi ed as the abuser's.

We also looked for potentially suspicious software, especially in cases where clients were concerned about spyware. For example, when we inspected client P13's laptop, we found a browser extension that she did not know about or recognize. Further research revealed the extension was capable of tracking her browsing activity, seemingly explaining her concerns (Section 4.1).

Programmatic spyware discovery. Spotting spyware manually has fundamental limits, particularly given the covert nature of many spyware tools [10]. We therefore created a custom tool, ISDi, that programmatically determines all the apps installed on Android or iOS devices, and lists them sorted according to a heuristic threat score that we developed (see [37]). Notably, these include dual-use apps that were designed for legitimate use cases but can be easily repurposed for abuse.

Across all consultations, ISDi agged 60 apps as potentially problematic. Ten of these were false positives (mistakenly agged as potentially dangerous), and in these cases the consultant explained the client did not need to be concerned with them. The 50 remaining were dual-use apps, and of these, all were recognized and desired by the victim except for one: an app that turned devices into remote home surveillance systems with WiFi, camera, and motion detection capabilities. We were able to check the purchase date of the app, which the client con rmed was during the time she was living with her abuser, and thus concluded her abuser appeared to have installed it. In

response to this nding, the client said, "That's so scary. Why would he do that to my phone? Why would someone use the phone as a camera?" (P9).

Another capability built into ISDi is detecting whether a device has been rooted or jailbroken, which would allow more sophisticated spyware, along with other increased risks. We detected one rooted device, which we learned had been purchased for the client and set up by her abuser. The client, who at the time was living in a shelter, visited us with this device initially wrapped in tinfoil, fearing that the abuser could be using it for tracking. After explaining the risks associated with the device, the client decided not to use the device any longer and not to take it back to the shelter.

4.3 Clients' reactions to the consultations

The clients who participated in our study expressed a range of feelings and reactions in response to our consultations. As some of the quotes above indicate, clients often expressed concern or surprise over discovered vulnerabilities, but they also were quite engaged in the process of understanding these vulnerabilities and potential mitigations.

Clients want to know more about technology. Perhaps the most common reaction that clients had at all phases of our consultation was to try and gain a better understanding of what we found, or about technology in general, by asking questions. Clients asked many questions about things they had heard elsewhere regarding tech safety and security, but they were unsure of the validity of the information. For example, one client asked, "So the tinfoil idea, does that protect devices from GPS tracking, or is that a myth?" (P22). Another said,

> Question. I read in one of the pamphlets that stated that's why I always turn my phone o it said, `Even when your phone is turned o , unless you can remove the battery, it's not really turned o .' Is that true?" (P11)

The prevalence of these kinds of general tech safety questions suggests that there is a real need for access to experts who can provide valid information and advice regarding tech security and privacy, even without our speci c assessments and device and account privacy checks.

Beyond asking general questions about tech safety, clients also had questions about speci c security or privacy issues that they had been experiencing with their devices. Many IPV survivors frequently change devices, phone numbers, physical addresses, and more, as they seek to cut ties with their abuser. However, these changes also frequently result in common security mechanisms (such as two-factor authentication) preventing them from changing these settings, or even completely locking them out of their own devices or accounts. For example, one client asked,

> I have a question. When I try to do a password reset, a lot of them, they want access to a number that I no longer have. So if I don't have that number, I can't reset anything? I had one number for many years, and I changed it." (P11)

Clients also asked detailed questions in response to speci c vulnerabilities that we discovered during our checks of their devices or accounts. For example, one client whose password had potentially been compromised asked,

> But what I'm saying is that, let's say I'm suspicious and so I change my password. Then does that pretty much take care of it, or would he somehow be able to gure out my password through whatever spy thing he had?" (P9)

Many of the clients' questions were valuable in helping us to assess their understanding of the vulnerability that had been discovered. They also created opportunities for us to have a conversation with the client to discuss what the vulnerability was, how we had discovered it, and what information the abuser might have as a result of it. In many cases, clients asked if there was any way to know

exactly what information that their abuser had about them. For example, one client whose cloud account showed the presence of an unknown trusted computer said,

> That's his computer. That was set up to my phone? Is there any way I can see what his access is through the [computer]? (P18)

In addition to asking questions about technology, clients also responded to our investigations by asking about actions they might take. We now discuss these in detail.

Clients want to take action. Many of the clients for whom we surfaced vulnerabilities were eager to take steps that might prevent their abuser from having access to their information, devices, or accounts. For example, one client whose passwords had potentially been compromised said, Yeah, I'm going to change my password on every single thing because (P7). Another client whose iCloud account showed an unknown trusted device asked us,

> Can I change that [iCloud] to disconnect from him completely, so that he has absolutely no access? . . . Can I delete this iCloud and then make a new [one]? (P18)

However, although many clients were eager to make immediate changes, we were careful to explain that it was important they spend time with their IPV professional to safety plan before making such changes. This is because an abuser who is used to having access to the victim's information might get angry and escalate the abuse (e.g., resort to physical violence) if that access is suddenly cut o . Indeed, a big part of our consultation design was to ensure that each client we met with was already receiving services from a quali ed IPV professional who would be able to provide safety planning support. In most cases the referring professional was not present, and this raised the issue of how to perform a hand-o of results that enabled appropriate safety planning.

Some clients were con dent about telling their IPV professional what we had discovered. For instance, the same client from the last example (whose iCloud had been compromised) said,

> I can call [my IPV professional]. Do you want me to try calling her again before I leave? I can call her and see when I can set up another meeting just to go over everything here. Basically, it is just the iCloud, no other suspicious apps. (P18)

Other clients worried that they would not be able to accurately represent to the professional the complexity of the tech entanglements that we had unearthed, and asked if we would speak with the professional on their behalf. One client said, I think it would be a good idea if you guys do it, just because my lingo may not be the correct language (P22). A couple of clients asked to schedule another consultation to help them e ect changes after safety planning occurred.

We helped clients immediately make changes during the initial consultation in two types of situations: (1) if the referring professional was present, and safety planning could occur immediately, and (2) if the client decided that they wanted to make changes to their digital accounts without waiting for their IPV professional. In these cases we ultimately respected the client's decision, in keeping with our client-centered approach. As one client said,

> No, I want to change everything now. Yeah. I don't care. I won't live like [this] . . . I prefer to change everything, and he gets mad . . . I have to focus on something else . . . If he does something, I'll call 911, and he goes to jail, and that's it. I'm tired. I'll nd out how to do this. I'll change the password. (P20)

Safety planning typically involved discussing with the client (1) what their abuser may know or discover if a change is made (e.g., the abuser would know their spyware had been discovered and deleted), (2) what information their abuser might lose access to as a result of any actions, and (3) given the client's particular situation, what their abuser may be likely to do as a result (e.g., confront the client in person). In some cases, the answers to these questions made the client feel con dent that they would be safe, and so they went ahead and made any desired changes. However,

in some cases, clients decided that they were not ready to make any changes, in which case we further discussed with them what information the abuser may continue to know or have access to. The changes we helped clients make included choosing new passwords, revoking access for unknown trusted devices, turning o location sharing, removing apps from devices, and more. We were careful to ensure that the client actually made the changes, not us. This was important not just for researcher safety but also as a mechanism for client empowerment and education: clients often asked additional questions as they made changes, creating opportunities for additional training.

Clients want reassurance and validation of their concerns. Beyond making changes to their accounts and devices in response to discovered vulnerabilities, several clients wanted us to provide reassurance about their situation. In fact, many clients were very happy when we did not find any evidence of tech abuse or compromise. As one client said at the end of the consultation, *So it looks like overall, you think that I'm okay?* (P9). Part of the reassurance that clients were often seeking was an acknowledgment that their situation was real and their concerns legitimate. After describing her situation, one client asked, *Whatever I said, did I sound crazy?* (P3). Other clients wanted to know if they were the only one experiencing these kinds of issues, or if we had seen others who might have had similar experiences. As one client asked,

> Can I ask you one thing? Is this a common situation that I'm having? Like nobody has a situation like this? . . . I'm trying to gure out if this is only me, that I'm having this kind of situation, or are there other people? . . . How many women are having this kind of situation? In the hundreds? (P27)

Clients mostly found the consultations valuable. Although we did not ask clients directly whether they thought the consultation was useful, or conduct post-consultation surveys (for client privacy reasons), we are optimistic that clients valued our consultations and that they are helping with the clients' as-yet unmet need for help dealing with tech abuse. Some clients who had forgotten to bring in all of their devices, or who could not remember their access credentials for all of the ones they did bring, asked if it would be possible to have another consultation. For example, one client asked if she could return another day to have a device checked, telling us, *I'd rather have peace of mind that it's not compromised, because he is very crafty* (P16). We took this desire for additional device checkups as a sign that clients found the consultation valuable. Many clients also expressed their gratitude at the end of the consultation and tried to refuse the compensation we o ered them. Several asked if our device scanning tool was available for them to use outside of the consultations if they later became suspicious. One asked,

> Is there a way . . . if I needed to nd out more in the future, to do a scan myself? Or how would somebody who isn't seeing you today be able to scan their device? (P9)

There were occasional exceptions to the general positive reactions we received. In a few cases, our consultations did not yield any plausible explanation for what the client was experiencing, which disappointed some clients. As one client aptly put it, *I think what's unfortunate is, although you're not nding anything, it doesn't make my experience any less real* (P11).

4.4 Our role as tech consultants

We now analyze our own roles as tech consultants in the complex, socio-technical systems found in IPV contexts. We begin by discussing how we carefully navigated interactions with clients within our understand-investigate-advise framework, before discussing how clients and IPV professionals perceived our role as a new node of support within IPV ecosystems more broadly.

Understand, investigate, and advise. One of our roles as consultants was to work collaboratively with clients (and IPV professionals) to disentangle the client's complex digital footprint and map

out account or device interdependencies that result in vulnerabilities. This process often focused on helping the client connect the dots between what they were experiencing or concerned about and how this might (or might not) relate to their security practices or account settings, including the impact of things they may have already tried to mitigate perceived tech problems.

We illustrate with an example that is representative of a few di erent client situations. The client's chief concern was that their abuser seemed to know information that they could only get if they had access to the client's accounts. To try and mitigate this problem, the client frequently changed her password, but further circumstantial evidence showed the abuser appeared to regain access. This made the client worry about the presence of spyware; however, our scans did not indicate any spyware currently installed. Discussions, though, revealed that although she used strong passwords and changed them regularly, she stored these passwords in les (e.g., notes or photos) that were synced with a cloud storage account. Our investigations revealed it was potentially compromised. We were then able to advise the client of the general risks associated with storing passwords in this way, as well as discuss with them steps they could take to revoke unauthorized access to the cloud account. In many such consultations, clients were relieved when they were able to connect the dots and discover a plausible explanation for their experiences. As one client said,

> Yeah, that's probably what he did. I'm pretty sure that's what it was . . . He could go log in and see any [information] that was under there. (P7)

In several cases, we were also able to discuss with a client why certain actions they had tried might be insu cient to combat the problem they were experiencing, and possibly suggest new strategies. For example, one client was receiving a large number of harassing calls from many unknown numbers that she assumed were all her abuser, but she did not have conclusive evidence. She expressed that she felt paranoid about receiving these calls and did not answer them. Prior to her consultation, she had responded by simply blocking each new number that called, telling us, If it's not in my directory, I block it (P21). We were able to explain to the client how, if it was the abuser, they would likely be able to continue harassing her via more and more spoofed phone numbers, and suggested she instead consider changing her phone number, which is the most e ective defense against call and text bombing that we are aware of.

Of course, when advising clients about possible steps they might consider to mitigate detected vulnerabilities, we played an important role in trying to ensure that they rst performed appropriate safety planning with an IPV professional. We did this by o ering to call the professional and suggesting that the client set up a meeting, or asking the client if they consented to the professional coming into the room immediately. Occasionally, we saw a need to intercede when a client wanted to do some action that we had just determined was not safe. For example, one client with a compromised iCloud account immediately took a screenshot showing an unrecognized login presumed to be the abuser, even though the screenshot would be immediately synced with that same compromised iCloud account. In this case, we suggested that the client delete the screenshot and also ensure it was removed from the Recently Deleted section of the Apple Photos app.

It was also important that we as consultants identi ed and discussed with clients when there were risks that could not be eliminated. For example, many clients faced ongoing risks emanating from their shared children carrying digital devices back and forth between the client and abuser. In many cases, children's devices were owned and had been set up by the abuser, which presented numerous risks. However, some clients were unable to get rid of these devices. As one said,

> I never wanted [my child] to have the phone. The courts ruled that [my child] is entitled to this phone [from the abuser]. I tried to get rid of this phone completely. I did not want any part of it. (P18)

In these situations, the best we could do was to discuss the potential risks of these devices with the client and to inspect the child's device, if available, e.g., to check for location tracking, while acknowledging that these devices continued to pose risks. Another opportunity to acknowledge the limitations of our consultations arose in situations where our tools failed to yield any plausible explanation for the client's concerns. These situations arose in 2 of our 31 consultations. For both cases, we discussed with the client how our tools were not foolproof (i.e., there may be some technical explanation that we missed), and also how there are many non-technical methods that abusers might use instead (e.g., physical stalking).

Tech consultants are seen as a new support node in the IPV ecosystem. Prior work examining the role of technology in IPV [32] highlighted the lack of trained technologists within these ecosystems. By offering our consultations within the FJC system, we found that we are increasingly viewed by many stakeholders as a new node of support for clients, which affects how clients and IPV professionals perceive our role as tech consultants.

For example, by integrating our intervention into the FJCs, we found that clients often assumed we could be trusted completely with all their devices, accounts, and data. All of the clients in our study did not hesitate to hand over and unlock their devices. We always asked for permission to touch or look at client devices and usually received responses such as *Yeah, go ahead. Do whatever you need to do* (P27). By working within the trusted FJC ecosystem, and through referrals by trusted IPV professionals, clients afforded us similar levels of trust as they did these advocates, even though they had never met us before.

We initially saw our role as discovering tech vulnerabilities and advising clients, and we expected IPV professionals would then help clients determine the best course of action. However, in practice, we found that IPV professionals often looked to us for advice about what was safe for clients to do. For example, during safety planning with a client, one IPV professional asked,

> *So when she's going into [locations] like these, what do you recommend for her to do to block off that location?* (IPV professional)

Thus, instead of a handing off to the IPV professional, safety planning with clients often ended up being a collaborative effort involving the consultant, IPV professional, and client. Similarly, we initially expected that legal professionals would be the ones to tell us what digital forensic evidence would be needed for use in a client's legal case. In reality, both clients and legal professionals often looked to us for advice about what should be documented and how. For example, one client asked us, *So how do I prove that he's doing all these things? What are the next steps?* (P27). In another case, a professional asked us, *Is this something that she can report to the police?* In these cases, we were careful to point out that we were not legal experts. Nevertheless, we often played a role in helping clients document evidence of tech abuse that resulted from our consultations.

Another way in which consultants became part of the services offered by the FJCs was by providing technology advice to professionals. On days when we visited FJCs, we let IPV professionals know that we were also available to answer questions or have discussions about technology. These informal drop-ins enabled professionals to ask questions regarding ongoing cases in which they were involved, including assessing whether they should refer particular clients to us for consultations. Along these lines, as IPV professionals have become more aware of our work, they have begun to spontaneously reach out to us whenever they have clients who are experiencing tech abuse or are in crisis, putting us into the role of first responders for tech abuse. For example, one professional reached out to schedule an urgent consultation, telling us,

> *Her ex-partner has used several apps and other programs to track her whereabouts, and she is in urgent need of a screening of her phone.* (IPV professional)

In some cases, IPV professionals have also reached out to us after our initial consultation with a client to request additional information and/or ongoing support. For example, one client changed her passwords multiple times after our consultation but kept seeing suspicious login activity on her account. Her IPV professional reached out to us and asked,

> I understand that, if spyware was installed, he could have been tracking keystrokes such that changing the passwords would not solve the problem, but in the absence of any spyware, I would have thought this would be over. So how could someone still be gaining access after changed passwords? (IPV professional)

We followed up with the professional over the phone and discussed possible explanations for this problem, also o ering a followup consultation to make any necessary changes for the client.

5 DISCUSSION

5.1 Challenges and issues intervening in IPV contexts

Researchers in HCI, CSCW, and other technology-related elds are increasingly pursuing agendas that aim to address large-scale social issues [6, 15, 16, 25, 44, 67]. As Dombrowski et al. point out [19], such systemic or wicked problems are challenging for researchers and designers to engage with due to their scope, scale, complexity, and political nature [27, 43]. They are also characterized by their lack of a clear objective answer or solution [51]. Our work deploying an intervention within the complex socio-technical systems encountered in IPV contributes a case study of how we, as technologists and interventionists, engage with the wicked problem of IPV, and our qualitative analysis o ers a detailed look at how IPV survivors experience such an intervention.

Of course, by intervening in these socio-technical systems as designers and tech consultants, we also change the realities of these systems themselves [24, 45, 53, 59]. In keeping with the principles of design justice, our work strives to view change as emergent from an accountable, accessible, and collaborative process, rather than as a point at the end of a project [13]. In our case, clients, IPV professionals, and consultants collaboratively work together to navigate the nuances of digital entanglements and tech abuse that clients experience, thereby changing the nature of the support services that are o ered to IPV victims. These changes impact the work and practices of multiple stakeholders and raise new ethical and sustainability questions, as we now discuss.

IPV survivors. Our interventions change the technology challenges and issues faced by IPV survivors, as well as their personal practices of digital privacy and security. For example, at the FJCs, many clients immediately trusted both us as consultants and our consultation tools and procedures. They readily unlocked their devices and gave them to us during consultations, potentially placing their concerns about tech abuse above their personal digital privacy concerns. We see similarities here to, for example, patient privacy in medical examinations, where clients engage in invasive procedures because they need aid from their doctors. The high level of trust clients placed in consultants speaks to their urgent need for tech assistance, but may result in security or privacy risks for the client should the consultant breach or abuse that trust. It also raises the importance of developing strong screening and training procedures for consultants to ensure they are trustworthy.

Our consultations also enable clients to ask questions and acquire new security practices. When we discovered speci c vulnerabilities for 14 clients, we engaged them in detailed conversations about tech safety and privacy, which may have resulted in new knowledge for clients and, in some cases, concrete changes to clients' digital accounts and devices, marking a change in their practices. However, we are aware that changing clients' tech safety and security practices may in turn change abusers' tactics and tools. For example, as clients learn to better protect the security of their online accounts (the most prevalent vulnerability that we found), abusers might turn to more sophisticated

spyware to surveil their victims. Thus, tech safety in IPV may turn into an arms race between victims and abusers as tactics and mitigation strategies evolve side by side.

As awareness of our clinical intervention spreads, we have also started receiving direct requests from IPV victims who want help with tech abuse problems but who are not clients of the FJCs. So far, we have referred them back to the FJC system, but they raise the question about what walk-in clinical models might look like for tech abuse. A key bene t of working within the FJCs is the ability to ensure proper safety planning with IPV professionals. For cases where there is no referring professional, it may be worth investigating how to safely perform some level of tech consultation. Otherwise, some IPV survivors may not be able to access our intervention at all.

Relatedly, a limitation of our work is that, by working within established IPV support services, we have interacted primarily with survivors who have already managed to physically leave their abuser (all but one of our participants no longer lived with their abuser). This study sample is clearly not representative of all people who experience IPV. In particular, there are a large number of IPV victims who are still living with their abuser, may be unable to get away, or are unable to seek help via an FJC. Additional work is needed to explore how we might safely provide assistance to victims at other stages of abusive relationships. For example, future research may examine how to adapt our protocols for online consultations (e.g., via anonymous chats) or self help. However, it will be critically important to address the safety aspects of such service models, since victims who are still living with their abusers may face greater risks of abuse escalation to physical violence.

IPV professionals. Prior work suggests that IPV professionals feel they do not possess su cient technology expertise to con dently identify or cope with tech abuse [32]. By intervening to provide tech assistance, our data suggests that we, as tech consultants, are rapidly being viewed as another node in the IPV support services o ered at FJCs. Where previously IPV professionals would search the Internet on their own for possible remedies to client tech problems, they now reach out to us. On one hand, giving IPV professionals ways to communicate with quali ed technologists will lead, we hope, to higher-quality advice and information for clients. On the other hand, it raises numerous questions as we consider how to sustain and, ideally, scale the intervention to meet demand.

The increased demand for consultations suggests that we need to think more expansively about potential deployment models and the role of IPV professionals. One approach would be to design a two-tier structure for tech interventions that includes: (1) improved front-line screening of clients for tech issues by non-technologist IPV professionals; and (2) referral models for consultations with tech consultants. For (2) we expect that our existing protocols will serve as a sound foundation.

For (1), future work will need to address how to better train non-technologist IPV professionals (e.g., case managers, lawyers) about performing tech abuse screenings and, as part of that, how to determine who would bene t from a consultation with a technologist. One might look to existing procedures in medicine and law for possible approaches to referring people to specialists. The vast majority of requests for consultations we received were agged as urgent by the referring professional. In our opinion, about half of these warranted a fast intervention by technologists, due to evidence of ongoing compromise of the client's accounts or devices uncovered during our consultations. The other consultations produced no tangible outcomes, though clients may have bene ted from us providing reassurance. Should there be resource constraints in terms of available technologist consultation slots, we might need to work with IPV professionals to design new triaging approaches analogous to those used in emergency rooms and legal clinics, paired with the necessary dedicated training for non-technologist IPV professionals to help perform such triaging. How to go about designing all those procedures and trainings remains an open question.

Us, as consultants and interventionists. In addition to the sustainability, scalability, and other challenges discussed above, intervening in IPV contexts also raises numerous ethical issues for us

as technologists and researchers. For example, we had to balance the concern that our interventions may cause some unexpected negative e ect (e.g., an escalation of abuse due to changes to a client's technology) with the fact that not intervening allows known, ongoing harms to continue unabated. We navigated this dilemma in part through guidance from IPV professionals, who routinely help clients deal with unknown situations, and by taking cues from clients themselves, many of whom have made multiple changes and gone to extreme lengths to cope with ongoing abuse. We also draw inspiration from feminist HCI [5] to point out that doing nothing in such situations potentially serves to reinforce the status quo and perpetuate regressive and harmful practices and structures.

Another ethical challenge we faced was the need to navigate our own biases, opinions, and intentions as technologists. In particular, our client-centered approach, in which clients are the ultimate authority on their own situations, sometimes clashed with our own beliefs about what actions were, in our view, security and privacy best practices. In one such case, after learning that the abuser had full access to the client's iCloud through her child's iPad, we recommended that a client create a new iCloud account. However, she was concerned about losing hundreds of dollars in iTunes music purchases and did not want to make the suggested change. In such situations, we are mindful of the need to prioritize the values and opinions of survivors above our own [5, 13] and keep in mind that they are the ones who will be directly impacted by the outcomes of any actions.

5.2 Implications for technology design

Adding and improving privacy and security interfaces. Clients' wide-ranging concerns about being tracked, monitored, and surveilled via technology, combined with the many questions they asked about technology security and privacy issues, suggests that IPV victims have both a strong need and a strong desire to be able to exercise meaningful control over their digital assets. Their struggle to do so suggests opportunities for tech platforms to provide improved control over and visibility into how people's accounts and devices are being accessed and used.

As a starting point, many popular platforms (e.g., Apple, Google, Facebook, Instagram) do provide privacy and security interfaces that are intended to give people information about, for example, trusted devices or recent login information (e.g., Google's `recent logins' interface). However, although such tools exist, which technically makes it possible for clients to investigate their digital assets on their own, none of our participants were aware of these interfaces or knew how to use them. This suggests that there are opportunities for tech platforms to make such interfaces generally easier to nd and use, perhaps through publicity, marketing campaigns, or improved visibility on platforms' home pages. In addition, platforms that do not provide such interfaces (e.g., Amazon, Outlook 365) should consider how they might do so e ectively.

Although clients were unaware of tech platforms' privacy and security interfaces, we did nd that they were useful for consultants conducting manual privacy checks of client accounts and devices. Indeed, the information provided by these tools led to the discovery or con rmation of account compromise for a number of clients, as described in Section 4.2. This shows how the privacy and security interfaces for popular websites and apps have, in the consultation context, taken on a distinct new purpose as diagnostic tools used by a third party, namely the consultant. To the best of our understanding, this is far outside the use cases envisioned by designers of these systems, and such usage presents interesting new design possibilities. For example, tech platforms might consider how to design such security features with the clinical consultation process in mind, perhaps providing richer details via an advanced interface designed speci cally for use in consultations. Such interfaces could include technically detailed forensic information (e.g., login times, IP addresses, granular location of login and other device identi ers) that would be highly

valuable in consultations. Of course, the design process should also consider the risks such changes might play given abuser access to the account, perhaps via IPV safety reviews as suggested by [38].

Helping people understand relationships between digital assets. Given the lack of knowledge that clients in our study had about who had access to their accounts and devices, there is also scope for platforms to improve the ways that they notify people about potential risks, such as new (or continued) device logins. They might also send more frequent con rmations or reminders to users when privacy-sensitive features like family sharing or location sharing are turned on. For example, currently Google sends monthly noti cation emails to an account whose location is shared with another person. Other platforms, such as Apple's FindMyFriends, do not send any noti cations to an account that is enrolled in location sharing.

More broadly, our ndings clearly show a need for new tools that help users build better mental models of information ows and authorization dependencies across their devices and accounts. Reminder noti cations are one such mechanism, but our interactions with clients suggests that misunderstanding of information ow is pervasive (e.g., images being synced across accounts, les accessible from di erent devices). Both users and consultants also need to better understand authorization dependencies what accounts or devices can be authorized to access a particular technology asset. Current approaches, such as con guration screens listing backup emails/phone numbers for recovering account access or which apps have been authorized to access an account's data are disjointed and poorly understood by clients.

One approach would be to design visualization tools that help users understand information ow and authorization dependency relationships. Our technograph can be seen as a pen-and-paper approach to doing so, but digital versions that extract con guration information from accounts to graphically depict information ows and authorization relationships would likely be more accurate and informative. In turn, companies could provide sharing summaries that provide users with guided tours that make sense of an account's information and authorization ows. Transitive cross-platform ows will be signi cantly harder to similarly visualize, since they would rely on compositions of security and sharing con gurations on distinct platforms. Nevertheless one can imagine building a tool that gathers such information to drive a visualization.

Such tooling could also be useful for helping simulate for users what will happen when they intervene via con guration changes. By showing graphically what accounts and kinds of information would be impacted, a client, perhaps with the aid of a consultant, could better appreciate the impact on the abuser's access, which is critical for e ective safety planning.

Life event mechanisms. Finally, as a more holistic approach to making changes to sharing and account access, platforms might consider providing a mechanism through which people could notify them about potentially impactful life events (e.g., breakups, divorce, etc.) in the same way that people, for example, notify companies about lost credit cards, possible identity theft, or change of address. There could then be a set of speci c steps or recommendations that tech platforms advise people to take to help them disentangle and secure their accounts after such a life change. In line with the principles of Universal Design [40], we anticipate that providing ways for IPV victims to gain meaningful control over their digital assets would likely lead to improvements for all users.

6 CONCLUSION

This paper described a qualitative analysis of a eld study that explores an approach to helping survivors of IPV with technology abuse, called clinical computer security. Data from face-to-face consultations with 31 IPV survivors, and professionals working on their behalf, showed that many participants faced ongoing tech abuse problems, and that our consultation protocol uncovered

important security vulnerabilities that survivors were unaware of. We discussed participants' experiences with our consultations and how they perceived our role as consultants and interventionists within the IPV ecosystem more broadly. We also re ected on the broader ethical issues that we faced intervening in complex IPV situations, including the work ahead that would be needed to sustain and scale our clinical computer security services for IPV victims. Finally, we discussed opportunities for the design of technologies that better support IPV victims.

7 ACKNOWLEDGMENTS

We sincerely thank all our participants and research partners, especially the ENDGBV and FJCs. This work was funded in part by NSF grant #1916096.

REFERENCES

[1] Mark S Ackerman. 2000. The intellectual challenge of CSCW: the gap between social requirements and technical feasibility. Human Computer Interaction 15, 2-3 (2000), 179 203.

[2] 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.

[3] 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.

[4] Jørgen P Bansler, Erling C Havn, Kjeld Schmidt, Troels Mønsted, Helen Høgh Petersen, and Jesper Hastrup Svendsen. 2016. Cooperative epistemic work in medical practice: an analysis of physicians' clinical notes. Computer Supported Cooperative Work (CSCW) 25, 6 (2016), 503 546.

[5] Shaowen Bardzell. 2010. Feminist HCI: taking stock and outlining an agenda for design. In Proceedings of the SIGCHI conference on human factors in computing systems. ACM, 1301 1310.

[6] Lynn Bickley and Peter G Szilagyi. 2012. Bates' guide to physical examination and history-taking. Lippincott Williams & Wilkins.

[7] Lindsay Blackwell, Jill Dimond, Sarita Schoenebeck, and Cli Lampe. 2017. Classi cation and its consequences for online harassment: Design insights from heartmob. Proceedings of the ACM on Human-Computer Interaction 1, CSCW (2017), 24.

[8] danah boyd. 2012. Truth, Lies, and `Doxxing': The Real Moral of the Gawker/Reddit Story. Wired (2012).

[9] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. Qualitative research in psychology 3, 2 (2006), 77 101.

[10] Rahul Chatterjee, Periwinkle Doer er, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 441 458.

[11] Citizen Clinic. 2019. https://cltc.berkeley.edu/citizen-clinic/. (2019). Online; accessed 2019.

[12] 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.

[13] Sasha Costanza-Chock. 2018. Design Justice: towards an intersectional feminist framework for design theory and practice. In Proceedings of DRS 2018 International Conference: Catalyst (2nd Edition). 529 541.

[14] Ronald J. Deibert. 2019. The Citizen Lab. https://citizenlab.ca/. (2019). Online; accessed 2019.

[15] Nicola Dell and Neha Kumar. 2016. The Ins and Outs of HCI for Development. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16). ACM, New York, NY, USA, 2220 2232. https://doi.org/10.1145/2858036.2858081

[16] Jill P Dimond, Michaelanne Dye, Daphne LaRose, and Amy S Bruckman. 2013. Hollaback!: the role of storytelling online in a social movement organization. In Proceedings of the 2013 conference on Computer supported cooperative work. ACM, 477 490.

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

[18] 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.

[19] Lynn Dombrowski, Ellie Harmon, and Sarah Fox. 2016. Social Justice-Oriented Interaction Design: Outlining Key Design Strategies and Commitments. In Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS

'16). ACM, New York, NY, USA, 656–671. https://doi.org/10.1145/2901790.2901861
[20] David M Douglas. 2016. Doxing: a conceptual analysis. *Ethics and information technology* 18, 3 (2016), 199–210.
[21] Anthony Dunne and Fiona Raby. 2013. *Speculative everything: design, fiction, and social dreaming*. MIT press.
[22] Louise Ellison and Yaman Akdeniz. 1998. Cyber-stalking: the Regulation of Harassment on the Internet. *Criminal Law Review* 29 (1998), 29–48.
[23] 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.
[24] NYC ENDGBV. 2019. NYC Mayor's Office to Combat Domestic and Gender-Based Violence. https://www1.nyc.gov/site/ocdv/about/about-endgbv.page. (2019).
[25] Sheena Erete, Aarti Israni, and Tawanna Dillahunt. 2018. An Intersectional Approach to Designing in the Margins. *Interactions* 25, 3 (April 2018), 66–69. https://doi.org/10.1145/3194349
[26] 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.
[27] Geraldine Fitzpatrick. 2003. *The locales framework: understanding and designing for wicked problems*. Vol. 1. Springer Science & Business Media.
[28] Geraldine Fitzpatrick and Gunnar Ellingsen. 2013. A review of 25 years of CSCW research in healthcare: contributions, challenges and future agendas. *Computer Supported Cooperative Work (CSCW)* 22, 4-6 (2013), 609–665.
[29] NYC FJCs. 2019. NYC Family Justice Centers. https://www1.nyc.gov/site/ocdv/programs/family-justice-centers.page. (2019).
[30] Sarah Fox, Mariam Asad, Katherine Lo, Jill P Dimond, Lynn S Dombrowski, and Shaowen Bardzell. 2016. Exploring Social Justice, Design, and HCI. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 3293–3300.
[31] 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.
[32] 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.
[33] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM.
[34] Lisa A Goodman and Deborah Epstein. 2008. *Listening to battered women: A survivor-centered approach to advocacy, mental health, and justice*. American Psychological Association.
[35] Lisa A Goodman, Kristie Thomas, Lauren Bennett Cattaneo, Deborah Heimel, Julie Woulfe, and Siu Kwan Chong. 2016. Survivor-defined practice in domestic violence work: Measure development and preliminary evidence of link to empowerment. *Journal of interpersonal violence* 31, 1 (2016), 163–185.
[36] 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.
[37] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *USENIX Security*.
[38] HeartMob. 2019. https://iheartmob.org/. (2019). Online; accessed 2019.
[39] Leigh Honeywell. 2019. Personal communication. (2019).
[40] Susanne Iwarsson and Agnetha Ståhl. 2003. Accessibility, usability and universal designâĂŤpositioning and definition of concepts describing person-environment relationships. *Disability and rehabilitation* 25, 2 (2003), 57–66.
[41] Maritza Johnson, Serge Egelman, and Steven M Bellovin. 2012. Facebook and privacy: it's complicated. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM.
[42] 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)*.
[43] J Kolko. 2012. Wicked problems: problems worth solving: a handbook and call to action. Ac4d. *Austin Center for Design, Austin* (2012).
[44] Neha Kumar and Nicola Dell. 2018. Towards Informed Practice in HCI for Development. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 99 (Nov. 2018), 20 pages. https://doi.org/10.1145/3274368
[45] John Law. 2004. *After method: Mess in social science research*. Routledge.
[46] Kaitlin Mahar, Amy X Zhang, and David Karger. 2018. Squadbox: A Tool To Combat Online Harassment Using Friendsourced Moderation. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, D401.

[47] 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.

[48] 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.

[49] 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.

[50] Wanda Pratt, Madhu C Reddy, David W McDonald, Peter Tarczy-Hornoch, and John H Gennari. 2004. Incorporating ideas from computer-supported cooperative work. *Journal of biomedical informatics* 37, 2 (2004), 128–137.

[51] Horst WJ Rittel and Melvin M Webber. 1973. Dilemmas in a general theory of planning. *Policy sciences* 4, 2 (1973), 155–169.

[52] Carl Ransom Rogers. 1959. *A theory of therapy, personality, and interpersonal relationships: As developed in the client-centered framework*. Vol. 3. McGraw-Hill New York.

[53] Victoria Sadler. 1999. The Politics of Technology: On Bringing Social Theory into Technological Design. *Technical Communication* 46, 2 (1999), 278–278.

[54] Safe Chat Silicon Valley. 2017. Safe Chat Silicon Valley. (2017). http://safechatsv.com/.

[55] Robert C Smith and Ruth B Hoppe. 1991. The patient's story: integrating the patient-and physician-centered approaches to interviewing. *Annals of internal medicine* 115, 6 (1991), 470–477.

[56] Sharon G Smith, Kathleen C Basile, Leah K Gilbert, Melissa T Merrick, Nimesh Patel, Margie Walling, and Anurag Jain. 2017. The National Intimate Partner and Sexual Violence Survey (NISVS): 2010-2012 state report. (2017).

[57] 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).

[58] Reem Talhouk, Kellie Morrissey, Sarah Fox, Nadia Pantidi, Emma Simpson, Lydia Emma Michie, and Madeline Balaam. 2018. Human Computer Interaction & Health Activism. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. ACM, New York, NY, USA, Article SIG15, 4 pages. https://doi.org/10.1145/3170427.3185369

[59] Alex S Taylor. 2011. Out there. In *The SIGCHI Conference on Human Factors in Computing Systems*. ACM, 685–694.

[60] TECC. 2019. Technology-Enabled Coercive Control Working Group, Seattle, USA. https://teccworkinggroup.org/. (2019). Online; accessed 2019.

[61] National Network to End Domestic Violence. 2017. NNEDV website. (2017). https:nnedv.org/.

[62] National Network to End Domestic Violence. 2017. Tech Safety App. (2017). https://techsafetyapp.org/.

[63] Stephen Viller. 1991. The Group Facilitator: A CSCW Perspective. In *Proceedings of the Second Conference on European Conference on Computer-Supported Cooperative Work (ECSCW'91)*. Kluwer Academic Publishers, Norwell, MA, USA, 81–95. http://dl.acm.org/citation.cfm?id=1241910.1241916

[64] 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.

[65] Rick Wash. 2010. Folk models of home computer security. In *Symposium on Usable Privacy and Security*. ACM, 11.

[66] 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.

[67] Jill Palzkill Woelfer. 2014. Engaging homeless young people in HCI research. *interactions* 21, 1 (2014), 54–57.

[68] Delanie Woodlock. 2017. The abuse of technology in domestic violence and stalking. *Violence against women* 23, 5 (2017), 584–602.

[69] Zijian Zhang, Jiamou Liu, Ziheng Wei, Yingying Tao, and Quan Bai. 2017. From Secrete Admirer to Cyberstalker: A Measure of Online Interpersonal Surveillance. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017 (ASONAM '17)*. ACM, New York, NY, USA, 613–614. https://doi.org/10.1145/3110025.3110065

A THE TECHNOLOGY ASSESSMENT QUESTIONNAIRE (TAQ)

Technology Assessment Questionnaire (TAQ)

Start with the most pressing concern widely expressed by clients thus far

- Do you worry that your device(s) is being used to track you?
  - Does the abuser show up unexpectedly or know things they shouldn't know?

Probe for risks of device compromise

- What devices do you use in your home or carry with you?
  (e.g., smartphone, iPad, tablet, desktop, laptop, kindle, echo, etc.)
- Do you currently (or have you in the past) share(d) your devices with your abuser?
- Is there any chance that your abuser has (or had) physical access to your devices?
  - Does (Did) your abuser ask or demand physical access to your devices?
- Who set up the screen locks or passwords on your devices?
  - Do you use fingerprint or facial recognition to unlock your devices?

Probe for risks from ownership-based attacks

- Do have a shared family plan?
- Do you or does someone else pay for your phone plan or Internet access plan?

Probe for risks of account compromise

- Who set up your email account or other online accounts?
- Have you ever shared any passwords with your abuser (or anyone)?
  - When did you last update your passwords for your email or other online accounts?
  - How do you remember your passwords?
  - Do you ever take photos of your passwords?
  - Is there a chance your abuser knows (or could guess) the answers to your password reset questions?
- Do you think your abuser has access to your accounts online?
  - Do you have an iCloud or Google account?
  - Do you think the abuser knows the password or has access to your bank account?
  - Do you think the abuser knows the password or has access to your email accounts?
  - Do you think the abuser knows the password or has access to your social media accounts? (Facebook, Instagram, WhatsApp, etc.)

Probe for risks from children's devices

- Do you have any children?
  - Do you share devices with your children?
  - Do you or does someone else pay for your children's devices?
  - Who gave your child their device?
  - Does the abuser have access to the child's device?
  - Does your child bring their device to visitation with the other parent?

Fig. 1. The current version of the Technology Assessment Questionnaire (TAQ).

B THE TECHNOGRAPH

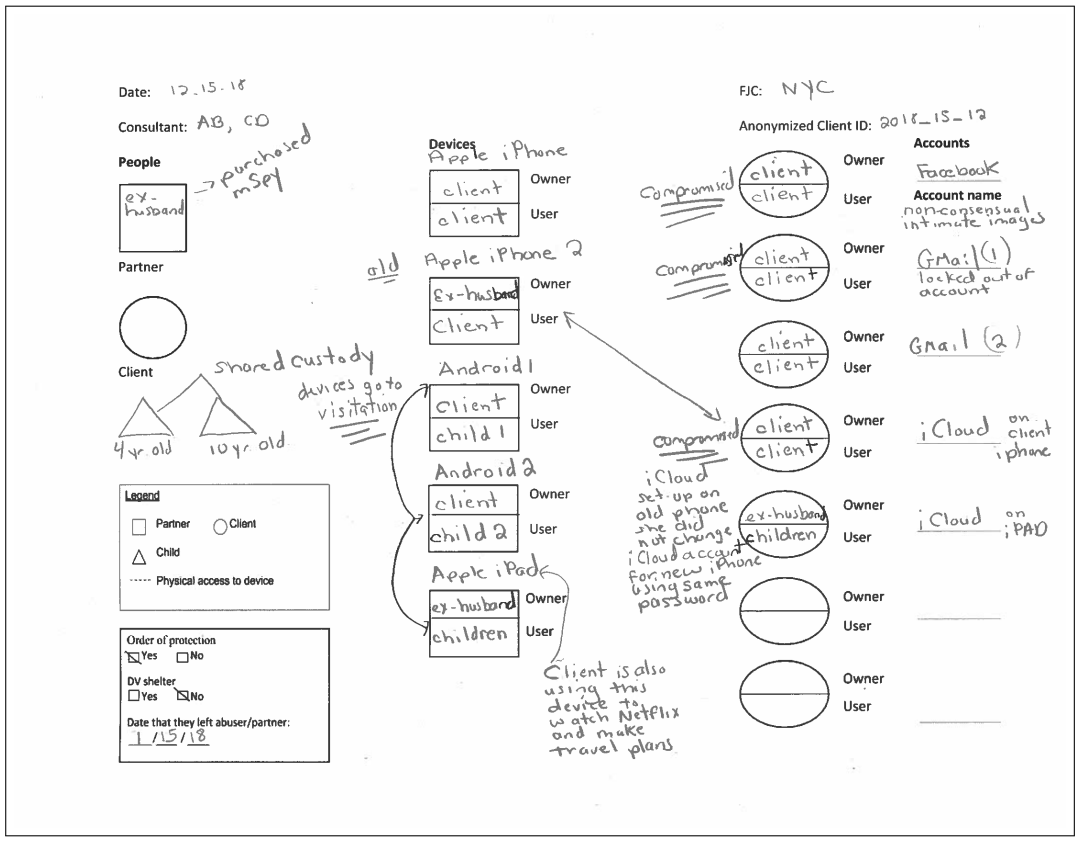

Fig. 2. An example technograph as it might have been filled out for a hypothetical client.