Clinical Computer Security for Victims of Intimate Partner Violence

Sam Havron[*,1] Diana Freed[*,1] Rahul Chatterjee[1] Damon McCoy[2]
Nicola Dell[1] Thomas Ristenpart[1]
[1] *Cornell Tech* [2] *New York University*

Abstract

Digital insecurity in the face of targeted, persistent attacks increasingly leaves victims in debilitating or even life-threatening situations. We propose an approach to helping victims, what we call *clinical computer security*, and explore it in the context of intimate partner violence (IPV). IPV is widespread and abusers exploit technology to track, harass, intimidate, and otherwise harm their victims. We report on the iterative design, refinement, and deployment of a consultation service that we created to help IPV victims obtain in-person security help from a trained technologist. To do so we created and tested a range of new technical and non-technical tools that systematize the discovery and investigation of the complicated, multimodal digital attacks seen in IPV. An initial field study with 44 IPV survivors showed how our procedures and tools help victims discover account compromise, exploitable misconfigurations, and potential spyware.

1 Introduction

As computers and other digital technologies take an increasingly central role in people's lives, computer insecurity has for some people become debilitating and even life-threatening. Activists and other dissidents are monitored [7, 23, 25, 26], journalists are harassed and doxed [10], gamers are subjected to bullying [9], and abusers are exploiting technology to surveil and harass their intimate partners [35]. Traditional security mechanisms most often fail in the face of such targeted, personalized, and persistent attacks.

A different approach for helping targeted individuals is what we call *clinical computer security*. The idea is to provide victims of dangerous attacks the opportunity to obtain personalized help from a trained technologist. Just like people visit doctors for health problems, seek out lawyers when suffering legal troubles, or hire accountants for complex tax situations, so too should victims of dangerous digital attacks have experts to assist them. But while these other examples of professional services have a long history leading to today's best practices, for computer security we are essentially starting from scratch: existing technology support services are ill-suited for helping victims in dangerous situations. The research challenge is therefore to develop rigorous, evidence-based best practices for clinical approaches to computer security, as well as design the supporting tools needed to help victims.

In this paper we explore clinical computer security in the important context of intimate partner violence (IPV). IPV is widespread, affecting one out of three women and one out of six men over the course of their lives [32]. Prior work has shown how abusers exploit technology to harass, impersonate, threaten, monitor, intimidate, and otherwise harm their victims [8, 14, 19, 20, 27, 35, 43]. Prevalent attacks include account compromise, installation of spyware, and harassment on social media [20,27]. In many cases digital attacks can lead to physical violence, including even murder [34]. Unfortunately, victims currently have little recourse, relying on social workers or other professionals who report having insufficient computer security knowledge to aid victims [19].

Working in collaboration with the New York City Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV), we designed, prototyped, and deployed a clinical computer security service for IPV survivors.[1] Doing so required not only developing first-of-their-kind protocols for how to handle face-to-face consultations while ensuring safety for both clients (the term we use for IPV victims in this context) and technology consultants, but also the design and implementation of new technical and non-technical instruments that help to tease apart the complicated, multifaceted digital insecurities that clients often face.

We designed a first-of-its-kind consultation procedure via a careful, stakeholder-advised process that made client safety paramount. Initial designs were refined over two months via 14 focus groups with a total of 56 IPV professionals, including social workers, police, lawyers, mental health professionals, and more. This led to substantive feedback and refinements,

[*] These authors contributed equally to the paper.

[1] Our initial and refined research protocols were approved by our institution's IRB and the ENDGBV leadership.

culminating in a consultation design that appropriately takes into account the socio-technical complexity of IPV and the unique risks that clients face.

Our consultation procedure starts with a referral from an IPV professional, and then proceeds through a face-to-face discussion where we seek to *understand* the client's technology issues, *investigate* their digital assets via programmatic and manual inspections, and *advise* them and the referring professional on potential steps forward. This last step, importantly, involves procedures for clearly communicating new found information about technology abuse so that professionals can help clients with safety planning. Supporting this understand-investigate-advise framework are a number of tools that we created, including: a standardized technology assessment questionnaire (the TAQ); a diagrammatic method for summarizing a client's digital assets called a technograph; succinct guides for helping consultants and clients manually check important security configurations; and a new spyware scanning tool, called ISDi, that programmatically detects whether apps dangerous in IPV contexts are installed on a client's mobile devices.

After completing our design process, we received permission to meet with clients in order to both help them and field test our consultation procedures and tools. Thus far, we have met with 44 clients and our consultations have discovered potential spyware, account compromise, or exploitable misconfigurations for 23 of these clients. The tools we developed proved critical to these discoveries, and without them our consultations would have been significantly less effective. For clients with discovered issues, we provided advice about improving security, in parallel with appropriate safety planning guided by case managers knowledgeable about their abuse history and current situation. Many other clients expressed relief that our consultations did not discover any problems.

Professionals at the FJCs have uniformly responded positively to our field study, and reported that the consultations are helpful to their clients. Demand for consultations has increased and we are performing them on an ongoing basis. More broadly, our tools, including ISDi, will be made open-source and publicly available, providing a suite of resources for testing the replicability of our clinical approach in other locations. Whether our approaches and methods can be useful for other targeted attack contexts beyond IPV is an interesting open question raised by our work. We discuss this question, and others, at the end of the paper.

2 Towards Clinical Computer Security

This paper considers targeted attacks in the context of intimate partner violence (IPV). Prior work indicates that IPV victims are frequently subject to technology abuse [8, 14, 19, 20, 27, 35, 43], and a taxonomy by Freed et al. [20] includes four broad categories: (1) ownership-based attacks in which the abuser owns the victim's digital accounts or devices, giving them access and control; (2) account or device compromise; (3) harmful messages or posts (e.g., on social media); and (4) exposure of private information online. Abusers use access to victim devices or accounts to setup dangerous configurations, such as adding their fingerprints to be accepted for device login, configuring devices to synchronize data with an abuser-controlled cloud account, or setting up tools such as Find My Phone to send location updates to an abuser's email address. Another avenue is installation of spyware apps that provide powerful features for monitoring devices [8].

Technology abuse in IPV is certainly complex in the aggregate, but even specific individuals suffer from complex, multifaceted threats. To concretize this, we give an example. For privacy reasons it is not any particular person's story. However, it is representative of many of the actual client situations we have encountered in our work.

Example scenario, Carol's experience: *Carol's now ex-husband subjected her to several years of increasing physical, emotional, and technology abuse before she obtained an order of protection, physically moved out, and filed for divorce. They are in a custody battle over their two children, ages four and ten, who live with the ex-husband part of the time.*

Carol knows that he installed spyware on at least one of her devices, because she found the purchase of mSpy on their joint credit card statement. Additionally, he had access to her private photos that he then posted on Facebook. He would also routinely, over the period of a year, "hack" into her online accounts, posing as her in efforts to further alienate her from her friends and family. He even locked her out of her GMail account by changing the recovery emails and phone number to his, which was devastating to her career in sales because it contained her business contacts.

Carol currently has five devices: a new Apple iPhone that is her primary device, two Android phones used by her children, an Apple iPad tablet bought for her children by her ex-husband, and a several-year-old Apple iPhone originally bought for her by her ex-husband. She routinely uses Facebook, a new GMail account (since her old one was stolen by her ex-husband), and a variety of other social media apps that are important for her work in sales.

This representative example highlights the complexities faced by IPV victims. Carol has a complicated *digital footprint* that includes a wide variety of devices and online accounts, some of which may be linked (e.g., different devices may have stored authentication credentials for different online accounts). She has complicating *entanglements*, meaning digital or personal relationships that may enable or complicate tech abuse, or render its mitigation more difficult. In Carol's case, the abuser has access to the children's devices, owns some of the devices in her digital footprint, and her need to use social media for her career limits options for preventing harassment via it. The complex timeline of events, such as when she physically moved out and when the children visit the abuser, may be directly relevant to the tech problems she is facing. Finally, there is also the risk that blocking digital attacks causes an *escalation* of abuse, such as triggering physical violence as the abuser seeks to regain his control.

One avenue for improving on the status quo is pursuit of new technology designs that better resist such targeted attacks. While doing so is very important, future designs will not help IPV victims in the near term. More pessimistically, it may in fact *never* be possible to rule out damaging attacks by highly resourced, determined adversaries against lower-resource victims. We therefore need complementary socio-technical approaches to helping victims.

Unfortunately, existing victim support services struggle to help with complicated tech abuse situations [19, 27]. The case workers, lawyers, police, and other professionals that work with victims report having insufficient tech expertise to help victims with digital threats [19]. There currently are no best practices for how to discover, assess, and mitigate tech issues [19]. Existing tools for programmatically detecting spyware are ineffective [8], and the state-of-the-art in practice is that professionals assume spyware on phones if a victim reports that the phone is acting strangely [20].

Commercial tech support services (e.g., Geek Squad [36] or phone stores) are unfortunately not a ready solution for addressing tech abuse. Prior work reports that victims occasionally use these services [19, 27], but that even when used they often fail to effectively diagnose problems [20]. We believe this is because commercial IT support professionals do not have context-specific training needed to identify and handle complex tech abuse situations prevalent in IPV. In the worst case, they put victims into more danger due to a lack of appropriate safety planning. Finally, victims with lower socio-economic status may find such services hard to access.

Clinical computer security. We target new approaches for victims to obtain personalized and appropriately contextualized support from a trained technologist. There are a handful of existing efforts from which we drew some inspiration. The Citizen Lab [13] and related Citizen Clinic [1] have been working for several years with targets of government persecution, a recent Technology-Enabled Coercive Control (TECC) clinic was established for IPV victims in Seattle [2], and individual computer security experts have long informally volunteered to aid those suffering attacks [24]. However, there has been little research into how such personalized security services should be systematically designed and deployed.

We propose an approach that we call *clinical computer security*. The goal is to develop, in a rigorous, evidence-based way, a set of best practices for how a technology *consultant* can assist a victim — called the *client* in such a service context — with digital insecurity. Best practices will need to encompass a range of issues, including how to setup and run clinics, recruit and train volunteers or paid professionals to staff them, deal with the many legal issues that will inevitably arise, and how consultations with clients should proceed. In this initial work we focus on designing and prototyping consultations, the fundamental element of any clinical approach. We discuss other aspects of running a clinic in Section 8.

The challenges faced in client consultations. As seen in Carol's example, individual IPV victims often experience a wide range of tech problems. They have a complex digital footprint, including multiple devices and online accounts, each of which can be a vector for abuse. They often have many nuanced entanglements. Existing tools for detecting spyware have a high false negative rate [8]. To improve outcomes for IPV victims, we need to design a protocol for face-to-face consultations that can integrate into existing victim support infrastructure, help us understand the client's problems from their point of view, discover tech risks they may not be aware of, and safely advise them about what steps they could take to improve their computer security.

Of course, we can look to other disciplines that use clinical interventions for guidance, including medicine, social work, mental health counseling, and even legal practice. These areas have long histories leading to today's best practices, including common interview procedures such as standards for psychiatric assessments [28] or client-centered advocacy [31]. However, none of these disciplines speak to procedures for computer security, so while we incorporate ideas from them when useful, overall, we need new approaches.

3 Methods, Client Safety, and Ethics

We designed a client consultation protocol and associated instruments to improve computer security outcomes for IPV victims via face-to-face discussions and both programmatic and manual investigations of their digital assets (i.e., their computing devices and online accounts). Here we discuss our iterative design methods that optimized for client safety.

IPV victims can be in dangerous and even life-threatening situations, and we made client safety and well-being central to our methodological approach. No consultation process will ever be perfect, in the sense that one could guarantee that all of the client's technology problems will be discovered, accurately assessed, and successfully mitigated. Indeed, the current status quo is reportedly missing many issues, accurately assessing few of them, and only sometimes properly mitigating them [19]. To make progress, we must develop research protocols that respect client well-being, are cognizant of safety risks, weigh the relative benefits of research to those risks, and, overall, minimize the potential for harm.

We therefore put into place a multifaceted strategy for performing this research responsibly. We partnered with the New York City Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV) [16], which runs Family Justice Centers (FJCs) [17] in each borough of New York City (NYC). The FJCs provide a diverse array of resources for IPV victims, including police, legal, mental health, housing assistance, and more. All research protocols were approved not only by our institutional IRB but also by the ENDGBV leadership.

Our consultation protocols went through a thorough, iterative design process that: (1) started with initial designs grounded in findings from prior work [19, 20, 27]; (2) a two-month process of iterative and incremental refinements driven by focus groups with relevant IPV professionals; (3) a review and approval process with the ENDGBV leadership of our refined protocols and instruments for client consultations; and (4) an ongoing refinement process that was responsive to needs that arose during client consultations.

This process maximized the amount of meaningful research we could do *before* interacting with clients. In step (2) we conducted 14 rounds of iterative design with a total of 56 IPV professionals. Each round involved a 60–90 minute focus group held at one of the FJCs, in which we summarized the current consultation design, demonstrated our methods, and gave participants copies of our questionnaires and materials. They were encouraged to edit, rewrite, and redesign them. We took detailed notes. Data analysis was performed immediately after each focus group, consisting of a detailed assessment of our notes with a specific focus on suggestions for improvements or changes. In subsequent sections, we give examples of quotes emanating from focus groups that help explain, or led to changes in, our consultation protocol. These quotes are illustrative and not intended to represent a comprehensive thematic analysis of the focus groups.

After nine rounds of changes based on participant feedback, we had several consecutive focus groups that did not elicit any new suggestions. We therefore determined our procedure and methods were ready for a review and approval process with the ENDGBV. This involved presentations to, and discussions with, ENDGBV leadership about our protocol. Ultimately, we and the ENDGBV concluded that it was ready for use with clients due to (i) the sufficiency of safety procedures we put in place to minimize potential harm to clients, and (ii) the fact that the ENDGBV leadership concluded that our research would benefit their clients. We discuss our safety procedures for consultations in detail in Section 6.

Finally, we note that safety issues extend also to the well-being of the participating researchers. In addition to the potential for vicarious trauma or other emotional strain, spyware could in theory leak recordings of consultations to abusers. We discuss self-care and researcher safety in Section 6.

4 A Consultation Protocol for IPV Victims

We created and refined a first-of-its-kind protocol for conducting a tech consultation in which a trained volunteer with expertise in technology meets face-to-face with an IPV victim. We refer to the volunteer as the tech consultant, or simply consultant, and the victim as the client. A diagrammatic overview of our consultation procedure appears in Figure 1.

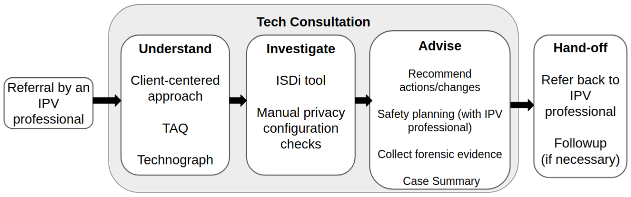

Tech Consultation
Referral by an IPV professional
Understand
Client-centered approach
TAQ
Technograph
Investigate
ISDi tool
Manual privacy configuration checks
Advise
Recommend actions/changes
Safety planning (with IPV professional)
Collect forensic evidence
Case Summary
Hand-off
Refer back to IPV professional
Followup (if necessary)

Figure 1: Summary of how a client participates in a tech consultation, beginning with a referral from an IPV professional.

We give a high level walk-through, and provide more details about various aspects of the procedure starting in Section 4.1. Throughout we give examples of how the iterative design process with stakeholders impacted our design.

We use a referral model that ensures safe integration of our consultations into NYC's existing survivor support services. Upon setting an appointment and meeting with a client, we use a procedure that we refer to as *understand-investigate-advise* (UIA). This emphasizes three important aspects of the consultation: understanding tech risks in the client's digital footprint, investigating their root causes, and providing advice about how they might improve their digital security.

To maximize the efficacy of the UIA procedure, we developed a number of non-technical and technical instruments to aid consultants, including: a technology assessment questionnaire, a diagrammatic approach called a technograph for mapping a client's digital footprint, guides for reminding consultants how to check security settings for common services and devices, and a software tool called ISDi (**I**PV **S**pyware **Di**scovery) that can safely detect the kinds of spyware reported as used in IPV settings by prior work [8]. We also developed a number of training materials, checklists, and associated protocols to help prepare consultants for meeting with clients. These instruments were refined via focus groups with professionals as well as in an ongoing manner as we gained experience working with clients.

4.1 Integration into Client Support Services

One of the first questions we faced is how to make tech consultations fit into the broader landscape of victim support services, such as legal, financial, and social services. Although consultants will be qualified to provide assistance with technology security and privacy, they will not necessarily be qualified to help with overall safety planning, legal advice, mental health, or other aspects of a client's case. It is therefore essential that other IPV professionals are able to assist the client before, during, and after a consultation.

To ensure all clients have appropriate support from an IPV professional, we use a **referral model** in which consultants only see clients that are referred to them by other IPV professionals for potential tech problems. Using a referral model has significant safety and procedural benefits over alternative models. In particular, the referring professional will know the client's background and abuse history and be qualified to help them safety plan around the results of the consultation (e.g., if it is safe to change their privacy settings, remove apps, etc.). If possible, and if the client is comfortable, we encourage the referring professional (or client case manager) to be present during the consultation so that they can also discuss their questions or concerns with the consultant.

Referral models have other benefits as well. They allow us to balance client anonymity with continuity of care, since the professional can serve as a safe communication channel between the consultant and client. This specifically enables consultants to perform **followups** for issues that cannot be fully investigated during a consultation. For example, we saw clients asking about esoteric or non-English apps, having browser extensions that are not on the extension market, and describing seemingly inexplicable tech situations. In such cases, we perform further research on the topic after the consultation, and communicate any discoveries back via the referring professional. If appropriate, the client may elect to participate in a second consultation, which happened a couple times so far in our work.

Regardless of followup requirements, when a consultation is complete (and with client permission) the consultant performs a **hand-off** procedure that communicates relevant findings to the referring professional. If the professional is in the room, this may happen at the end of the consultation. Otherwise, it happens via email or phone call. This hand-off is vitally important. First because it facilitates proper safety planning, as we discuss later in the section. In addition, it provides some reassurance to clients potentially frightened by a consultation's discoveries. As one professional described, our hand-off procedure:

> *"...might help the client feel a little bit more comfortable. 'Oh my gosh, I'm being tracked. At least I know there's an officer that can help me with this situation.' You're also aware of what's going on as a screener, as well as a case manager. I have three different backups. I think it was very well done."* (P36, Case Manager)

4.2 Understand-Investigate-Advise Procedure

When the client arrives for a consultation, we follow standard IPV advocacy practices and take a **client-centered approach** [31], which assumes the client knows best regarding their own situation and will be the one to make decisions. One professional described client-centered practice as:

> *"having a conversation with the client and ... letting the client formulate their decisions, their answers. [Professionals] cannot provide them with [answers] because they're the only ones who know what risks are being posed."* (P36, Case Manager)

Therefore, taking a client-centered approach, the consultant begins by asking the client what their main concerns are and/or what caused them to seek out a consultation. We refer to these as their chief concerns[2] and a primary goal of the consultant is to try to accurately identify them. For example, we heard clients express fear that spyware was installed on their devices, that their "phones were tapped", or that their abuser had access to information they should not have (e.g., a client's photos). In some cases the chief concerns are not very clear and take some gentle questioning to ascertain.

From this starting point, the tech consultant will utilize a wide range of instruments and tools that we have created to (1) **understand** the client's digital footprint and entanglements to identify potential avenues for harm; (2) **investigate** their devices, apps, and services to look for, and assess the root cause(s) of, their tech problems; and (3) **advise** clients on how they might move forward. See Figure 1.

Understanding footprint and entanglements. Prior work on tech and IPV [14, 19, 27, 34, 43] indicates that there are no best practices or standard procedures for asking about tech risks or understanding the root cause(s) of client concerns. The lack of standardized procedures may contribute to serious, on-going tech abuse being overlooked. We therefore created several instruments that help systematize the discovery and assessment of tech problems in IPV.

To systematize problem discovery, we created and refined a Technology Assessment Questionnaire, or **TAQ** (Figure 5 in the Appendix). We started with questions that aimed to uncover common problems surfaced in prior work [20], such as risk of device/account compromise if the abuser knows or can guess the client's passwords (e.g., their password is their child's birthday), or ownership-based risks, when the abuser is the legal owner of the client's devices or accounts. Feedback from focus groups helped us refine question wording, and include additional questions that professionals thought would be helpful. As one example, we received many suggestions on the importance of asking about children's devices. As one professional told us,

> *"[For parents] with younger kids, I think another question that might be important is asking if your children go on visits and if they take their electronics with them on visits."* (P40, Social Worker)

We added five questions about risks with children's devices. This feedback was particularly helpful, as we saw several cases in our field study of children's devices being the likely avenue by which the abuser had access to client data.

To support a client-centered approach, the TAQ is designed to be used as a reference to ensure consultants cover important topics, rather than as a prescribed interview format. The consultant lets the client lead the conversation and discuss

[2] In medicine, this would be called a chief complaint, but we feel that 'concern' is more client-centered.

topics they find important, which often touches on a subset of the TAQ. The consultant uses the TAQ to remember to raise remaining topics that the client may not have thought about. We arrived at this approach after early feedback from professionals that it is more empowering to let clients drive conversations, rather than peppering them with questions.

A challenge that came up in early consultations is building a mental map of the client's digital footprint and entanglements. Carol's example in Section 2 illustrates the potential complexity of client technology use. In the field, clients often came with half a dozen devices, many accounts, an involved abuse timeline, and various pieces of (often circumstantial) evidence of account or device compromise (e.g., the abuser keeps tracking or calling them despite changing phones). It is easy for consultants to lose track of relevant details.

We therefore created the **technograph**, a visual map loosely inspired by genograms, a technique used by clinicians in medicine and behavioral health to map family relationships and histories [22]. The technograph uses shapes and symbols to visually document relationships between (1) devices, (2) accounts, and (3) people (usually the client's family). Drawing connections between entities gives the consultant a clearer picture of potential sources of compromise. An example that may have been created discussing Carol's situation appears in Figure 6 in the Appendix.

The technograph is particularly helpful to identify when abusers may have indirect access to a client's digital assets. For example, two-factor authentication for iCloud accounts can be bypassed if a child's device is a contact for the account. Another example is when family plans synchronize data across devices and accounts. The technograph allows tracing these potential indirect access routes more easily.

Investigating devices, accounts, and services. After using the TAQ and technograph to construct a clearer picture of the client's situation, the next phase of the consultation is to thoroughly investigate devices, accounts, or services that may be compromised by the abuser. We created tools that investigate in two ways: (1) by scanning the client's mobile devices for spyware or other unwanted surveillance apps using a new IPV Spyware Discovery (ISDi) tool that we built, and (2) by manually checking the privacy configurations of the client's devices, apps, and accounts. We discuss each in turn.

As we detail later, most clients have hundreds of apps on their devices. In addition to the threat of spyware-capable apps being installed surreptitiously, many otherwise legitimate apps may be configured by the abuser to act as spyware. For example, Google maps can be configured to update an abuser about the client's location, and while it provides various notifications that tracking is ongoing, their effectiveness is uncertain. We therefore have a dichotomy between unwanted and wanted apps, with the mere presence of the former being sufficient for a safety discussion whereas the latter require investigation into their configuration.

Detecting unwanted apps manually via the user interface (UI) will not work: many IPV spyware apps can effectively hide their presence from the UI [8]. Indeed, current state-of-the-art practice by non-technologist professionals is to use circumstantial evidence to conclude spyware is installed, e.g., if a phone acts "glitchy" it most likely has spyware and should be reset if not discarded [20]. We therefore constructed an IPV Spyware Discovery (**ISDi**) tool for detecting unwanted apps on a client's iOS or Android devices. It also checks if the device has been jailbroken (for iOS) or rooted (for Android), which may indicate that dangerous spyware is installed. With the client's permission, the consultant uses ISDi to programmatically obtain via USB connection the apps installed on their devices, highlighting ones that are known to be risky in IPV. Should the device be detected as rooted/jailbroken or any risky apps found, the consultant can discuss whether the client rooted the phone, recognizes the app, etc.

Our focus groups with professionals helped us iterate on the user flow and understand how best to integrate the tool into client consultations. We learned that clients and professionals want to view and understand the steps required to use the tool as well as visually examine the scan results. Professionals expressed concern about communicating to clients appropriately about privacy issues. One professional suggested that, during a consultation, we say that:

> *"We will see and go through every application on your phone, we will not see any information in your social media, texts, photos. We will only see the names of all the applications but not see anything inside any of the apps and give an example, such as, if you have WhatsApp, we will not see any conversation inside."* (P41, Case Manager)

Focus groups also led us to realize that both clients and consultants are consumers of the ISDi UI (see Figure 2). We therefore avoided language that would be too confusing or scary to a client. Finally, while we have not yet done a thorough user study of the tool, we have begun some initial user studies with IPV support organizations (e.g., TECC [2]) interested in integrating ISDi into their own procedures. We discuss this further in Section 8.

That leaves checking configurations of common apps that are often wanted but potentially dangerous, as well as checking built-in system services (e.g., "find my phone" features), account backup mechanisms, and authentication lists (e.g., registered fingerprints), all of which may be sources of vulnerability. The same holds for online accounts deemed important by the client (e.g., email and social media accounts). Unfortunately, checking the privacy of these accounts cannot be easily automated, not only due to lack of device or web interfaces to support querying this kind of data, but also because one needs to understand the context and have the client help identify dangerous configurations. For example, in several cases we saw that the client's Facebook or GMail accounts had been accessed by devices the client could confirm as the abuser's.

To assist the consultant with these **manual investigations**, we constructed simple-to-follow guides for popular apps, device settings, and online service settings. For instance, our Google privacy configuration guide lists steps to check a device's login history, location sharing, photo sharing, and Google Drive backup settings. On iCloud we check family sharing, backups to iCloud, and if the abuser still has access to the account. We continue to expand the list of apps and services for which we have guides in response to ongoing work with clients, and currently cover Android (including Google maps and GMail), Apple (including iCloud and location sharing), Facebook, Instagram, and Snapchat. Unfortunately such guides may become out-of-date if software updates change configuration features. Future work on how to sustainably keep guides up-to-date will be needed (see Section 8).

Another benefit of performing manual investigations during consultations is that they serve as impromptu computer security training for clients, which prior work indicated is sorely needed [19]. In fact, many clients we met with did not know about security configuration features, and we were able to show them for the first time that, for example, they could tell what devices were logged into their GMail or Apple accounts. Clients often asked followup questions about security best practices during this part of the consultation, leading into an open-ended discussion about computer security.

Advising clients on potential next steps. In the final phase of the consultation, the consultant combines information gleaned from the understanding and investigation phases to assess the client's situation and, based on this assessment, discuss with the client (and professional, if present) what might be causing tech problems the client is experiencing. If the investigation phase yields any spyware, risky software, or privacy problems with the client's accounts and devices, these are discussed calmly with the client, including how the breach may have happened and potential actions that might remedy the situation. In these cases, the consultant can offer the client a printout that explains what was found and how it may be causing problems (Figures 10 and 11 in the Appendix).

Before taking actions or changing any settings, it is essential that the client discuss their consultation results with a professional to perform **safety planning**. Ideally the professional should be familiar with the client's situation and abuse history, since this is necessary to highlight potential safety issues related to tech abuse. One professional said:

> *"Safety planning is such an individualized thing. I can think of some cases where it would be advantageous to leave the spyware on. I can think of some where we would want it gone immediately. If you can, just find a way to integrate it into the normal safety planning protocol."* (P37, Paralegal)

If the client's case manager is not present, the consultant asks the client if they would like to contact their case manager and/or receive immediate assistance from another on-site professional. Thus, even if the consultation has identified tech problems that are the likely causes of the client's concerns, in many cases, the client may leave the consultation with their devices and accounts unchanged. For a few clients we met with who had complicated scenarios, we encouraged them to schedule a follow-up consultation via their professional, so we could help them further after safety planning.

Consultations also provide new opportunities for collecting **forensic digital evidence**. The need for clients to document evidence of tech abuse is an issue that legal professionals discussed at length in our focus groups. If properly collected, such evidence may help a client secure an order of protection or aid a criminal investigation. Although clients may want to delete suspicious apps or reconfigure settings, our protocol has the consultant discuss with clients the potential benefits of documenting any discoveries before taking action. We asked professionals about how to handle forensic evidence, and they suggested various approaches, such as:

> *"I would definitely take photos. Because ultimately [a detective] will be investigating that report, but I will definitely take photos, write down the name of the app on my report."* (P39, Police Officer)

We therefore settled on the expedient approach of having the client (or a lawyer acting on their behalf) take a photo or screenshot of any discovered spyware, evidence of compromises, etc. As suggested in the quote above, this is actually the standard of evidence currently, at least in family court, and several clients we met with have ongoing court cases in which they plan to use evidence discovered via our consultations.

In many cases the consultation will not yield any tech problems or causes for concern, in which case the consultant may reassure the client that, at least, our approaches did not find any problems. We are careful to not dismiss any problems that remain unaddressed or unexplained by our consultation. If additional investigation is warranted, the consultant explains to the client that they will do more work and follow-up via the referring professional (as explained in Section 4.1).

Finally, at the end of a consultation, the consultant completes a **case summary** that documents (1) the client's chief concerns (in their own words), (2) the consultant's assessment of problems, (3) the results of the ISDi scan and manual configuration check-ups, and (4) advice or recommendations discussed with the client. This case summary is for internal use only[3] and provides useful documentation for the consultant (or other consultants) that can be used should the client request another consultation or need followup.

[3] In some contexts such written documentation may be ill-advised due to the potential threat of hostile subpoena by lawyers working for the abuser. In our work, FJC professionals felt this threat was remote since our consultations take place within a research study that maintains client anonymity.

4.3 Replicability

An important question for our consultation protocol is how to ensure a standard of care that can be maintained across different locations and by different consultants. Many of the tools we created help by systematizing the assessment and investigation of tech problems. To complement these, prior work in disease diagnosis [15], surgery [42], and aviation [11] suggests that simple checklists are a valuable tool for systematizing procedures. Checklists help consultants follow a systematic procedure despite the complexity of many client cases, from both an emotional and technological standpoint. We created three checklists: one each for before, during (Figure 9 in the Appendix), and after the consultation.

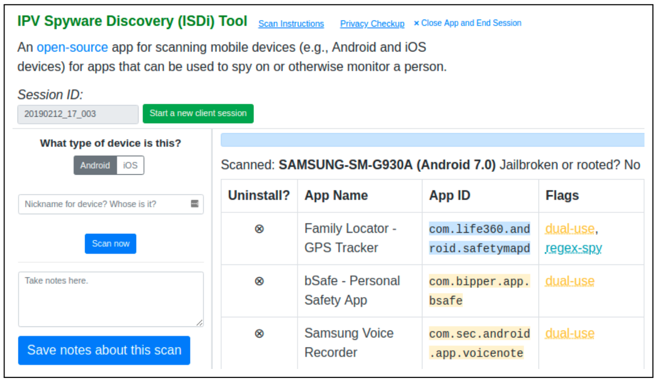
We also developed a process for training researchers involved in consultations. We wrote a 13-page training manual that includes a detailed description of our protocol with example situations. It also discusses consultant emotional well-being and safety considerations (e.g., that consultants not give their full names until after spyware scans are complete). Training included reading and understanding this manual, along with guided introductions to our instruments, including ISDi.

To gain experience in face-to-face consultations before interacting with clients, we performed mock consultations in which researchers role-play as clients (including setting up, beforehand, a realistic scenario possibly involving spyware or other misconfigurations) and others role-play as consultants (that do not a priori know the scenario). After each mock consultation, the group analyzes how it went, revealing the scenario and constructively discussing how to improve. These are valuable for consultants to gain confidence in their ability to handle consultations as well as for the research team to gather feedback on the usability of various instruments.

Although clearly more research can be done to further refine our instruments, our field evaluation, discussed in Section 6, indicates their immediate practical value. We have publicly released all training materials, instruments, and open-source tools as resources that other advocacy organizations might find useful in their work supporting survivors[4]. We have already been collaborating with the TECC group in Seattle [2], sharing materials and getting feedback. They have adopted some TAQ questions for use in their clinical settings, and we are working towards prototyping ISDi at their clinic.

5 The IPV Spyware Discovery (ISDi) Tool

We now discuss the technical design and testing of ISDi, our IPV Spyware Discovery tool designed for IPV contexts. While technologically ISDi currently only uses, relative to modern anti-virus tools, simpler techniques such as blacklists and other heuristics, the innovation is in tailoring it to IPV: (1) flagging apps that in other contexts are not necessarily dangerous and, importantly, (2) mitigating potential discoverability by existing IPV spyware. Both issues necessitated a new tool, as existing ones fail on both accounts.


Scan Instructions
Privacy Checkup
× Close App and End Session
Start a new client session
What type of device is this?
Android
iOS
Nickname for device? Whose is it?
Scan now
Take notes here.
Save notes about this scan

IPV Spyware Discovery (ISDi) Tool

An open-source app for scanning mobile devices (e.g., Android and iOS devices) for apps that can be used to spy on or otherwise monitor a person.

Session ID: 20190212_17_003

Scanned: **SAMSUNG-SM-G930A (Android 7.0)** Jailbroken or rooted? No

Uninstall?	App Name	App ID	Flags
⊗	Family Locator - GPS Tracker	com.life360.android.safetymapd	dual-use, regex-spy
⊗	bSafe - Personal Safety App	com.bipper.app.bsafe	dual-use
⊗	Samsung Voice Recorder	com.sec.android.app.voicenote	dual-use

Figure 2: Screen capture of the ISDi tool's main interface after scanning an Android testing device.

Regarding (1), in IPV harmful apps may include both spyware and what are called dual-use apps: otherwise legitimate apps that may be repurposed to act as spyware. We use the term 'IPV spyware' for both types of apps. Prior work showed how existing tools do not detect dual-use apps [8], whereas ISDi was designed to flag all spyware apps, including dual-use apps. Regarding (2), installing an existing anti-virus app is detected by current spyware, potentially endangering victims, while ISDi was designed to be more covert.

ISDi is a Python application with a browser-based user interface (Figure 2) that is used by the consultant to scan a client's devices and identify potentially harmful apps. The tool shows the scan results and serves as a starting point for discussion with the client about any discovered apps. During the investigation phase of a consultation, the consultant, with the client's permission, helps connect the client's device via USB to a laptop running ISDi. A benefit of this design architecture is that it does not require an app to be installed on the device, making it minimally invasive and leaving little to no trace of its execution. We discuss the safety of connecting to client devices below. Further details about how ISDi works are provided in Appendix A.

Detectability of ISDi. A key design consideration is that ISDi does not endanger victims due to being detectable by abusers. As discussed above, we chose to not make ISDi a downloadable app since we know some spyware reports any new apps that are installed. Instead we use the USB interface to connect the device to a laptop running ISDi.

In theory a sophisticated spyware tool might be able to detect ISDi's use of USB interfaces on iOS or Android. Therefore, we conducted additional risk assessments. We installed six highly capable, overt spyware apps found by Chatterjee et al. [8] on an iPhone 6 (running iOS 11.4) and also on a rooted Moto G4 Play phone (running Android 6.0.1). The six

[4] https://www.ipvtechresearch.org/resources

apps are: mSpy, Cerberus, FlexiSpy, SpyToApp, SpyZie, and Trackview. We inspected the features and descriptions of the less sophisticated apps reported on in [8], and decided they were unlikely to support detection of USB connections.

For each of the six considered spyware apps, we created an account (simulating the role of an abuser) and manually investigated capabilities that might allow the app to detect the scanning process (including those tailored to rooted Android devices). We then simulated normal use of the device for several minutes (e.g., opening apps, scrolling) and ran ISDi while network connectivity was enabled. We repeated this process with network connectivity disabled for the scan (and then re-enabled), the intuition being that spyware apps exfiltrate device activities and data to an external cloud-based account configured by the abuser, only some of which may be monitored in real time. We examined the information that the abuser obtains in both cases, and found that for five of the apps there was no way to infer that ISDi was used.

The remaining app, Cerberus, allows exfiltrating system logs on Android, although this capability must be manually invoked by the abuser. These system logs include entries about USB connections to the device and that the device connected to a power source, but nothing beyond that. A technically sophisticated abuser aware of our tool and who carefully analyzed these logs might suspect, but would not have conclusive evidence, that the device was scanned.

Finally, spyware might reveal that the client came to an FJC, and there have been reports of abusers physically confronting victims at FJCs or shelters [20]. However, our consultations and ISDi do not exacerbate this risk given that our clients already visit FJCs for other reasons.

Data collection. Although it is possible to use ISDi without collecting any data, for research and safety reasons we choose to store some information, including the list of apps on a device. Importantly, we do not collect any personally identifiable information or content, such as phone number, emails, photos, etc. See Appendix A for more details.

6 Field Study

After developing and refining our consultation protocol and instruments, we performed a six-month field evaluation with IPV survivors. The study was conducted in collaboration with the ENDGBV, who helped recruit participants, provided safe space for consultations, and ensured the availability of IPV professionals to help with safety planning. Before beginning our study we obtained ethics approval for all procedures from our university's IRB and from the ENDGBV.

Recruitment. We distributed fliers to all five FJC locations (one in each borough of NYC). These fliers advertised the study as a way for clients to obtain a tech safety and privacy consultation, making both clients and professionals aware of the opportunity. Interested clients were asked to speak with their case manager who, after consulting with the client, created a referral and an appointment with our team. Consultations were typically scheduled for days when our team arranged to be at the FJC, with a minimum of one and a maximum of four consultations on a single day. At the suggestion of ENDGBV staff, we gave participants $10 compensation to cover the cost of transportation to/from the FJCs.

Procedure. Consultations took place in a private room at one of the FJCs. 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 (ISDi scan, manual privacy checks), and a third (when available) to take notes. Consultations were done individually.

Clients scheduled for a consultation were advised to bring any digital devices that they used or that they wished to have checked. However, two participants did not bring all their devices to their first consultation and therefore made an appointment to return so as to have additional devices checked. Thus, two clients participated in two consultations.

Consultations lasted between 30 minutes and two hours. We began by introducing the team members to the client, explaining the purpose of the study, outlining the activities that would be performed, and discussing the data that would be collected about them and from their devices. We then obtained the client's verbal consent to participate. We also asked participants for permission to audio record the consultation for data collection purposes and received permission to record 36 out of 46 consultations. If the participant did not want to be audio recorded, we instead took detailed notes.

After receiving the client's consent to participate, we followed the consultation procedure detailed in Section 4, including questions from the TAQ, constructing a technograph, scanning the client's devices with ISDi, and performing manual privacy configuration checks. Whenever possible, we suggested it may be advantageous for the client to have their case manager or another IPV professional present during the consultation so they could assist with safety planning and/or documenting relevant findings. In total, 16 out of 44 clients had a professional present during their consultation. After performing all procedures and discussing relevant findings with the client (and professional, if present) we thanked the client for their time. For clients requiring followup, we discussed what that followup would be and confirmed the relevant professional to contact when the followup was complete.

Data collection and analysis. We collected detailed handwritten notes and audio recordings (when permitted) that document each consultation, including client answers to TAQ questions, discussion of their digital footprint, details of manual privacy checks, results from ISDi device scans, the advice or recommendations discussed with the client, and any followups that were done. All audio recordings were professionally transcribed and collated by consultation with the relevant handwritten notes, completed technograph, and ISDi data.

We manually went through all this data multiple times to carefully summarize each consultation and produce the descriptive and aggregate statistics presented in Section 7. The data was stored securely with controls limiting access to only the subset of the research team that performed analysis.

Safety protocols. As discussed in Section 3, IPV presents a sensitive landscape within which to conduct research and survivors are a vulnerable, at-risk population. Our research procedures were carefully designed to protect clients' privacy and safety. For example, we did not ask participants to sign a consent form since we did not want to know or collect any identifying information (e.g., names), and all communication with clients took place through the referring professional, including scheduling and any post-consultation followups.

Although we offered participants a variety of printed handouts to help them understand their digital safety and privacy, we explained there may be risks with taking such materials home, especially if they still lived with their abuser, since someone may discover they had received a consultation. In addition, since changing privacy settings or uninstalling surveillance apps could lead to potentially dangerous escalation of abuse, whenever possible we encouraged participants to have a trusted IPV professional present during their consultation. When this was not possible, we made sure that another experienced case worker was available to help develop safety plans that accounted for any detected tech abuse and/or discuss new protection strategies that participants may want to adopt.

We also considered safety and well-being for our research team. Part of our training included ways to balance the need to properly inform participants about who we were and our affiliation, while avoiding giving out detailed identifying information about the individual researchers. For example, we introduced ourselves by first name only. This was because of the risk that spyware on devices was recording conversations.[5] In addition, working with IPV survivors and hearing their stories may be mentally and emotionally challenging. We regularly met as a team after consultations to debrief and encouraged team members to discuss their feelings, experiences, or anything they were struggling with. Moreover, an experienced IPV case worker was available at all times to speak with researchers and help them process any upsetting experiences that occurred during the consultations.

7 Results of the Field Study

The main goal of our study was to evaluate the utility of our consultation protocol for IPV victims. Our tools and instruments uncovered important, potentially dangerous security problems that we discussed with clients and professionals. This preliminary data suggests our consultation protocol provides benefits. Given the small sample size taken from a single city, we warn that our results should not be interpreted as statistically representative of problems faced by IPV survivors. We discuss limitations of our results more in Section 8.

For the sake of client anonymity, we necessarily cannot report on the full details of our consultations. Instead, we give aggregate results, or when we discuss a particular situation we only do so in a way that makes it coincide with widely reported IPV technology abuse situations, as per prior work [8, 14, 19, 20, 27, 35, 43] and our experiences.

Participants and devices. We conducted a total of 46 consultations with 44 IPV survivors (43 female, 1 male) who were all clients at the FJCs. Two clients received second consultations (at their request) to scan additional devices. All participants were adults and one still lived with their abuser.

As shown in Figure 3 (left table), clients brought a total of 105 devices to the consultations. Of these 82 were Android or iOS and we scanned 75 of these with ISDi. Two unscanned devices were iPhone Xs, which initially caused an error in ISDi when Apple changed the format of device IDs (updates to ISDi fixed this for subsequent scans). In two cases, ISDi could not scan a very old iPhone, potentially due to an error in the libimobiledevice tool we use to communicate with devices. One iPhone was not scanned due to a client leaving early and two other phones were not scanned either because the client was locked out of the device or stated they were not concerned about scanning it. All devices that were not scanned with ISDi were checked manually, except two where clients were locked out of the device (a phone and laptop).

We performed manual checks on 97 out of 105 devices brought in by clients. Clients brought a number of devices for which we did not have a protocol for manual privacy check up, including Internet-of-Things devices such as Amazon Echos, gaming systems, a Blackberry phone, and a flip phone. We performed a best-effort inspection in such cases, except the flip phone for which the client had no privacy concerns.

Participants' chief concerns. Clients expressed a range of chief concerns, as shown in Figure 3 (middle table). The descriptions here, such as "abuser hacked accounts" reflect terminology used by clients. A relatively large number of clients (20) described experiences that suggest abusers had access to clients' online accounts (often described as "hacking") or reported evidence indicative of such access (e.g., abuser knows information only stored in an account). The second most prevalent chief concern (18 clients) were general concerns about their abuser tracking them or installing spyware, but without specific reasons for suspecting it. Other clients were concerned that their location was being tracked, their phone was acting suspiciously, and more. Finally, a few clients wanted to learn more about tech privacy and had no specific concerns about tech abuse directed towards them.

Chief concerns were often connected to the security issues we detected, discussed more below. For example, chief

[5] We explored other ways to protect researchers, such as leaving client devices outside or placing them in sound-insulated containers or Faraday bags, but these proved impractical.

Clients & Devices	
Clients seen	44
Consultations performed	46
Devices seen	105
Devices manually inspected	97
Devices scanned w/ ISDi	75
Median devices per client	2
Max devices per client	7
Median apps per scanned device	170

Chief Concerns	
Worried about tech abuse/tracking/spyware	18
Abuser hacked accounts or knows secrets	20
Worried abuser was tracking their location	10
Phone is glitchy	10
Abuser calls from unknown numbers	9
Unrecognized app on child's phone	1
Money missing from bank account	1
Curious and want to learn about privacy	4

Detected Issues	
Clients w/ vulnerabilities	23
Clients w/ unsolved problems	2
Clients w/ no problems detected	19
Potential spyware detected	3
Potential password compromise	14
Presence of unknown "trusted" devices	12
Shared family/phone plan	4
Rooted device	1

Figure 3: Summary of field study results. **Left:** Breakdown of the number of clients seen, consultations performed, and devices encountered. **Middle:** The chief concerns, as described by the clients (some had multiple chief concerns). **Right:** The problems detected during consultations, including vulnerabilities, security risks, and spyware (some clients had multiple problems).

concerns involving illicit access to accounts were often best explained by poor password practices, family sharing, or confirmation of account access by abuser devices. In one case the chief concern was entirely unrelated to the discovered security issue, however. All this confirms the importance of both identifying the chief concerns, but also using instruments and procedures that may surface unexpected problems.

Security vulnerabilities discovered. For 23 of 44 clients (52%), our consultations identified important security risks, vulnerabilities, or plausible vectors for tech abuse. Before describing our findings, it is important to note that, in most cases, we do not have definitive proof that the vulnerabilities discovered are the root causes of clients' problems. For example, if a client's password is the name of a child they share with the abuser, or if their phone is part of a shared family plan, these provide plausible theories for, but not hard evidence of, how compromises may be occurring.

Results from ISDi: ISDi flagged a total of 79 apps as problematic across all device scans. The majority of these (61) were dual-use apps, with "find my phone" and child monitoring apps the most prevalent categories. For all but one of these dual-use apps, discussions with clients confirmed that they recognized the apps and were aware of their presence. For one dual use app, the client said that they did not install or recognize the app, which was a controller for remote home surveillance systems with WiFi, camera, and motion detection capabilities. We treated this case as a true positive result. The other 18 apps detected by ISDi were false positives (i.e., clearly not relevant to IPV) that the consultant easily dismissed as such. The number of false positives in any individual consultation was low, the maximum number of flagged apps on a client's device was five. This meant that, thus far, we have not had any issues with consultants being overwhelmed by large numbers of apps flagged by ISDi.

The relatively low rate of actual spyware detection may be because, as discussed below, many abusers are seemingly able to surveil clients via compromised accounts, and so may not need to install spyware. In addition, almost all clients no longer lived with the abuser, had changed or reset their devices since leaving (which would remove spyware in most cases), and for many devices the abuser no longer had physical access needed to (re-)install spyware. Finally, ISDi detected that one client's Android tablet was rooted. Subsequent discussion revealed that the abuser bought this tablet for the client, had physical access to it during the relationship, and had insisted the client log into her accounts with it. As a result of our conversation, the client decided to stop using the tablet.

Results from TAQ and technograph: For many clients, we discovered security vulnerabilities through combined use of the TAQ, technograph, and/or manual privacy checks. In some cases, the TAQ and technograph were the primary (or only) way to uncover a potential problem. For example, four clients reported that they were still part of a shared family plan or that their abuser pays for their phone plan, vulnerabilities that could give the abuser access to, for example, the location of the client's device and call and text history. Another common problem that the TAQ and technograph revealed for 14 clients was the use of passwords that the client said were known, or could be guessed, by their abuser. In several of these cases, a compromised password provided a plausible explanation for how the abuser may be gaining access to the client's accounts.

Results from manual checks: Combining TAQ and technograph information with subsequent manual privacy checks often yielded evidence of malicious account access. For example, during manual checks of iCloud account settings for four clients, we discovered that their iCloud accounts listed "trusted" devices that the client either did not know or recognized as belonging to the abuser. Similarly, manual checks of client email and social media accounts showed unknown or abuser device logins for another eight clients.

iCloud and email account access, whether by password compromise or via unauthorized "trusted" device access, also yielded plausible explanations for a range of other problems. For example, three clients reported that they kept written records of passwords for all their accounts in files that were then synced with their compromised iCloud, potentially resulting in the abuser obtaining all these passwords. Similarly, several clients emailed copies of their new passwords to themselves via potentially compromised email accounts. Another prevalent avenue for compromise that we saw happened when clients used a compromised account as the backup account for other services (e.g., social media), with clients unaware of how this might result in abuser access to these services.

For two clients, manual checks of laptops revealed browser extensions that the clients did not install or know about. In one case, the extension was “off store” (not available via the official Chrome Web Store), may have been sideloaded (installed via developer mode), and had permission to read and write all browser data. We regarded this as possible spyware. For the other case, the extension is available via the Chrome Store and is used to monitor access to web content. This extension provides a plausible explanation for the client’s chief concern, which was that her abuser knew about her online activities, and we regarded it as probable spyware.

No problems detected. For 21 out of 44 clients, our instruments did not surface any evidence of potential tech issues. For 19 of these, the lack of discovered problems was reassuring and many left the consultation visibly relieved and more at ease. However, in two cases, the consultation’s inability to address their chief concerns left the client unsatisfied. In these cases we performed follow-up research, including reaching out to other tech experts for second opinions about their concerns (in an anonymized fashion) but unfortunately still have no plausible explanation for what they were experiencing.

Hand-off and followup. For the 23 clients with discovered problems and two clients with unresolved issues, we conducted a hand-off in which we discussed our results with the referring professional. For 12 of these, the professional was onsite and hand-off occurred immediately. For the other 13, we followed up with the professional via email and/or a phone call. Although many clients did not resolve discovered problems immediately because of the need to safety plan, they said that it was helpful and empowering to at least know how the abuser was plausibly obtaining information about them.

Eleven cases required further research after the consultation. Six of these were client requests for information about specific apps we were unfamiliar with (e.g., can app X track my location?). For the remaining five we found something during the consultation that needed further analysis to assess its danger. In 10 cases, the consultant researched the issue at length and provided a comprehensive answer to the referring professional within a few days of the consultation. In the remaining case, we could not provide a satisfactory explanation for what the client was describing even after significant research, which we explained to the referring professional.

8 Discussion

Although the results from our field study are preliminary, they suggest that our consultation protocol is already valuable to clients in dangerous situations. Encouragingly, the ENDGBV have asked our team to schedule more consultations with clients at the FJCs. This in turn raises new open questions about how to sustain and scale our clinical computer security approach. In this section we discuss: (1) limitations of our current study; (2) open questions that it raises about how to realize the vision of clinical computer security for IPV victims more generally; and (3) open questions that our work raises about clinical approaches to computer security beyond IPV.

Limitations. This first study on clinical computer security interventions has several limitations that we acknowledge. First, our study was restricted to a single municipality and our participants were not representative of all people who suffer IPV. Although New York City has a large and diverse population, and our sample does include socioeconomic and cultural diversity, all but one of our participants were women, all but one were no longer living with their abuser, and the majority had been in heterosexual relationships. As a result, our study may fail to capture some of the nuances associated with abusive relationships for LGBTQIA+ people or those who may still live with their abuser.

Another limitation is our sample size. Although 44 clients may be sufficient to verify the utility of our consultations, it certainly does not yield statistically significant estimates of, for example, likelihood of spyware or other harms being seen in practice. Further, our study context purposefully biases our sample towards victims that are specifically worried about tech problems. Still, our results provide guidance on what a tech clinic is likely to see, and our experiences are consistent with prior work on tech attacks in IPV [20, 27].

Our consultations may not catch all issues, either due to consultant error (e.g., forgetting to ask a TAQ question) or technical error (e.g., ISDi mislabeling an app). Indeed, one of the fundamental challenges faced in this area is dealing with complex, multifaceted attacks, and it is not possible to be perfect. That said, our new approach vastly improves over the current status quo in practice, which is essentially nothing. Moving forward, future research will need to assess if, and how, our protocol and instruments impact client lives in the longer term, determining, for example, whether our interventions measurably decrease illicit account accesses.

Should a client change their behavior as a result of our consultations, abusers may change behavior, retaliate against the victim, or otherwise escalate abuse. We designed our protocols to try to minimize the potential for this, but no procedures can eliminate such risks entirely. That said, we are in active communication with FJC leadership and have not received any indication that a client has faced retribution as a consequence of participating in a consultation.

Clinical computer security for IPV. Our work focused on client consultations, which are a fundamental component of realizing our vision of clinical computer security. Given the success of our initial field study, we are faced with a range of open questions. The most obvious is that our design and evaluation so far did not perform in-depth investigation of issues related to scalability and sustainability.

A sustainable computer security clinic will likely need a supporting organization, outside the scope of a research study, to handle recruitment, screening, and training of sufficiently many volunteer consultants (or paid professionals, should there be funding to pay them). Although the assessments and materials we developed in this work will help with training future tech consultants, they do not yet speak to challenges that are outside the context of the consultation. In a referral model like the one we used, just scheduling consultations took many hours per week and, more broadly, how best to organize delivery of clinical computer security for IPV victims raises a host of questions for future research.

As a financially sustainable recruitment strategy, we might draw on existing models like pro-bono legal services [30], and initial conversations with tech professionals and companies suggest that some may be willing to offer their time free of charge. (This model is used by the TECC clinic [2].) Another approach is student-run clinics, similar to law school legal clinics [12] or medical school free clinics [37]. In any such model, it will be essential to develop strong protocols for screening consultant applicants, particularly to ensure that abusers are prevented from enrolling as consultants. Advocacy groups have protocols for screening applicants, and one could start by adopting these. In parallel, future research will be needed to localize clinical techniques to geographic locations with different support organizations and laws.

Another pressing issue is maintenance of instruments. ISDi's coverage currently relies on labor-intensive updating of blacklists, based on web crawling and manual analysis. Like malware detection in other contexts, maintaining accuracy over time and staying ahead of emerging threats is an immense challenge [40]. It is also important to consider the longer-term implications of making ISDi's existence and methods public. While current spyware does not infer ISDi was used, if it becomes widespread enough to become a target, spyware developers might turn to more sophisticated methods that monitor USB-related system processes. Similarly, spyware vendors may start attempting to avoid detection. As such, we keep ISDi's blacklist private, allowing access via legitimate requests from those working to help victims.

Our other instruments will also require updating at various time intervals. By design, the TAQ should maintain relevance for quite a while to come, requiring updating only when technology changes suggest new, broad classes of threats we must consider. But our manual investigation guides for checking security or privacy settings may need to be updated more frequently as companies change their products. Future work might evaluate the right balance between generalizability and actionability of such guides (c.f., [19]), or infrastructure for maintaining them (e.g., expert crowdsourcing [29]).

Clinical computer security beyond IPV. IPV is not the only context in which victims suffer targeted, persistent, and personalized attacks. Some examples include the dissidents, activists, and NGO employees targeted by nation-state hacking campaigns [7, 23, 25, 26], or the gamers [9], journalists [10], politicians [6], and researchers [21] who are at high-risk of being harassed online [18, 33]. As in IPV, in all these cases the attacker wants to harm their particular target. There is also an asymmetry between the victim and attacker, with the latter having more resources, time, and/or technological sophistication. Indeed, in some cases the adversary in these other contexts has significant technical prowess.

Clinical approaches to computer security may be of utility in these other contexts. In the near term, adapting our techniques to other communities of victims similar to IPV — such as victims of elder, parental, or child abuse, or victims of sex trafficking (which are also served by FJCs) — could constitute important research directions. Despite the similarities, research will be needed to understand how the nuances emanating from particular circumstances or demographics change best practices for clinical interventions.

Further afield are contexts that are less similar to IPV. For example, those targeted by government agencies as mentioned above might benefit from systematized clinical approaches. One could perhaps start with the work done by the CitizenLab [13] and Citizen Clinic [1], and determine to what extent, if any, our methodologies for stakeholder-driven design could help improve clinical interventions.

9 Conclusion

This paper lays out a vision for clinical computer security and explores it in the context of IPV. Through an iterative, stakeholder-driven process, we designed a protocol for conducting face-to-face tech consultations with victims of IPV to understand their tech issues, investigate their digital assets programmatically and by hand to discover vulnerabilities, and advise on how they might proceed. Our preliminary study with 44 IPV victims surfaced vulnerabilities for roughly half our participants, including account compromise, potential spyware, and misconfiguration of family sharing plans. Our consultations also provided advice and information to victims and professionals on ways to document such discoveries and improve computer security moving forward. Our clinical approach provides immediate value, while also laying a foundation for future research on evidence-based refinements to clinical tech interventions in IPV and, potentially, beyond.

Acknowledgments

We would like to sincerely thank all our study participants, the Family Justice Centers, and the NYC ENDGBV. This work was funded by the NSF through grants CNS-1717062 and CNS-1558500, and by gifts from Comcast and Google.

References

[1] Citizen clinic. https://cltc.berkeley.edu/citizen-clinic/.

[2] Technology-enabled coercive control working group, Seattle, WA, USA. https://tecc.tech/.

[3] iOS jailbreak detection (OWASP). https://git.io/fj4te, 2017.

[4] Libimobiledevice: a cross-platform software protocol library and tools to communicate with iOS devices natively. https://www.libimobiledevice.org/, 2017.

[5] Android debug bridge (adb). https://developer.android.com/studio/command-line/adb, 2019.

[6] Maggie Astor. For female candidates, harassment and threats come every day. https://www.nytimes.com/2018/08/24/us/politics/women-harassment-elections.html, 2018.

[7] S. Le Blond, A. Cuevas, J. Ramón Troncoso-Pastoriza, P. Jovanovic, B. Ford, and J. Hubaux. On enforcing the digital immunity of a large humanitarian organization. In *2018 IEEE Symposium on Security and Privacy (SP)*, volume 00, pages 302–318.

[8] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.

[9] Despoina Chatzakou, Nicolas Kourtellis, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Athena Vakali. Hate is not binary: Studying abusive behavior of #gamergate on twitter. In *Proceedings of the 28th ACM Conference on Hypertext and Social Media*, HT '17, pages 65–74, New York, NY, USA, 2017. ACM.

[10] Gina Masullo Chen, Paromita Pain, Victoria Y Chen, Madlin Mekelburg, Nina Springer, and Franziska Troger. "you really have to have a thick skin": A cross-cultural perspective on how online harassment influences female journalists. *Journalism*, 2018.

[11] Robyn Clay-Williams and Lacey Colligan. Back to basics: checklists in aviation and healthcare. *BMJ Qual Saf*, 24(7):428–431, 2015.

[12] Robert J. Condlin. "tastes great, less filling": The law school clinic and political critique. *Journal of Legal Education*, 36(1):45–78, 1986.

[13] Ronald J. Deibert. The Citizen Lab. https://citizenlab.ca/.

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

[15] John W Ely, Mark L Graber, and Pat Croskerry. Checklists to reduce diagnostic errors. *Academic Medicine*, 86(3):307–313, 2011.

[16] NYC ENDGBV. NYC mayor's office to combat domestic and gender-based violence. https://www1.nyc.gov/site/ocdv/about/about-endgbv.page, 2019.

[17] NYC FJCs. NYC family justice centers. https://www1.nyc.gov/site/ocdv/programs/family-justice-centers.page, 2019.

[18] Antigoni-Maria Founta, Constantinos Djouvas, Despoina Chatzakou, Ilias Leontiadis, Jeremy Blackburn, Gianluca Stringhini, Athena Vakali, Michael Sirivianos, and Nicolas Kourtellis. Large scale crowdsourcing and characterization of twitter abusive behavior. *CoRR*, abs/1802.00393, 2018.

[19] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 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):Article 46, 2017.

[20] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018.

[21] Virginia Gewin. Real-life stories of online harassment — and how scientists got through it. https://www.nature.com/articles/d41586-018-07046-0, 2018.

[22] Philip J Guerin and Eileen G Pendagast. Evaluation of family system and genogram. *Family therapy: Theory and practice*, pages 450–464, 1976.

[23] Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill, and Ronald J Deibert. Targeted threat index: Characterizing and quantifying politically-motivated targeted malware. In *USENIX Security Symposium*, pages 527–541, 2014.

[24] Leigh Honeywell. Personal communication, 2019.

[25] Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda. A look at targeted attacks through the lens of an ngo. In *USENIX Security Symposium*, pages 543–558, 2014.

[26] William R Marczak, John Scott-Railton, Morgan Marquis-Boire, and Vern Paxson. When governments hack opponents: A look at actors and technology. In *USENIX Security Symposium*, pages 511–525, 2014.

[27] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 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*, pages 2189–2201. ACM, 2017.

[28] APA Work Group on Psychiatric Evaluation. *Practice Guidelines for the Psychiatric Evaluation of Adults*. The American Psychiatric Association, third edition, 2016.

[29] Daniela Retelny, Sébastien Robaszkiewicz, Alexandra To, Walter S. Lasecki, Jay Patel, Negar Rahmati, Tulsee Doshi, Melissa Valentine, and Michael S. Bernstein. Expert crowdsourcing with flash teams. In *Proceedings of the 27th Annual ACM Symposium on User Interface Software and Technology*, UIST '14, pages 75–85, New York, NY, USA, 2014. ACM.

[30] Deborah L Rhode. Cultures of commitment: Pro bono for lawyers and law students. *Fordham L. Rev.*, 67:2415, 1998.

[31] Carl R Rogers. Significant aspects of client-centered therapy. *American Psychologist*, 1(10):415–422, 1946.

[32] Sharon G Smith, Kathleen C Basile, Leah K Gilbert, Melissa T Merrick, Nimesh Patel, Margie Walling, and Anurag Jain. The national intimate partner and sexual violence survey (NISVS): 2010-2012 state report. 2017.

[33] Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 Internet Measurement Conference*, IMC '17, pages 432–444, New York, NY, USA, 2017. ACM.

[34] Cindy Southworth, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. A high-tech twist on abuse: Technology, intimate partner stalking, and advocacy. *Violence Against Women*, 2005.

[35] Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. Intimate partner violence, technology, and stalking. *Violence against women*, 13(8):842–856, 2007.

[36] Geek Squad. Geek Squad services. `https://www.geeksquad.com`, 2019.

[37] Lindsey Stephens, Nicole Bouvier, David Thomas, and Yasmin Meah. Voluntary participation in a medical student-organized clinic for uninsured patients significantly augments the formal curriculum in teaching underrepresented core competencies. *Journal of Student-Run Clinics*, 1(1), Jun. 2015.

[38] San-Tsai Sun, Andrea Cuadros, and Konstantin Beznosov. Android rooting: Methods, detection, and evasion. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 3–14. ACM, 2015.

[39] Jing Tian, Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bates, and Kevin Butler. SoK: "Plug & Pray" Today – Understanding USB insecurity in versions 1 through C. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 1032–1047. IEEE, 2018.

[40] X. Ugarte-Pedrero, D. Balzarotti, I. Santos, and P. G. Bringas. SoK: Deep packer inspection: A longitudinal study of the complexity of run-time packers. In *2015 IEEE Symposium on Security and Privacy*, pages 659–673, May 2015.

[41] Zhaohui Wang and Angelos Stavrou. Exploiting smartphone usb connectivity for fun and profit. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 357–366. ACM, 2010.

[42] Thomas G Weiser, Alex B Haynes, Angela Lashoher, Gerald Dziekan, Daniel J Boorman, William R Berry, and Atul A Gawande. Perspectives in quality: designing the who surgical safety checklist. *International journal for quality in health care*, 22(5):365–370, 2010.

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

A More Details about ISDi

How ISDi works. ISDi uses the libimobiledevice tool [4] for iOS or Android Debug Bridge (adb) [5] for Android to programmatically access the connected device. On Android, the device must be configured to allow USB debugging, which is done by enabling developer mode for the scan and revoking it again after the scan is complete. When a scan is initiated, ISDi pairs with the connected device and queries it for a list of all installed apps, including those that are hidden from the app drawer on Android (c.f., [8]). ISDi then runs additional queries on the device to obtain the OS version, hardware model, and manufacturer. It also performs heuristic checks to infer if the device is jailbroken (iOS) or rooted (Android). ISDi displays information about the outcome of these checks via the tool's UI, along with a list of all installed apps with potentially dangerous apps listed first. We compute each app's threat score by combining several heuristics.

First, we created a blacklist of potential IPV spyware and dual-use apps using techniques from Chatterjee et al. [8]. To ensure the list was not stale, we re-ran their measurements several times and added the results to the blacklist. We applied the machine learning classifier used in [8] to remove the obviously irrelevant apps. However, we did not manually prune the list further to reduce the falsely flagged apps, as during consultation a consultant can check those apps and ignore if not relevant for IPV. The most recent update was shortly before we initiated meetings with clients. Our current blacklist contains over 500 iOS and $5,000$ Android apps. A second heuristic is a set of regular expressions that app names are checked for, including substrings such as "spy" or "track". Lastly, on Android, ISDi checks whether any apps were installed outside of the Play Store. A threat score is then computed for each app so that the apps can be listed in decreasing order of potential risk.

Clicking on an app name in ISDi's UI displays more information about that app, including installation date, developer description of the app, requested permissions, and when permissions were last invoked (on Android). ISDi is also capable of uninstalling apps (after appropriate safety planning) via its interface, which is especially useful for hidden apps on Android that cannot be located using the device's UI.

ISDi is not perfect and may have both false positives and false negatives. The former are less dangerous, and in our experience were easily dealt with by the consultant in the field. False negatives are of course potentially dangerous, and so we purposefully designed ISDi to have a low false negative rate by allowing for more false positives.

ISDi collects the following information of each app: the app ID, permissions, installation date (Android only), and package files (Android only). ISDi also generates and stores a keyed cryptographic hash of the device's serial number. The latter is useful to ensure we can determine if we scan the same device twice, since clients may have multiple consultations, without explicitly storing the device identifier. Collected data is linked to a random client identifier. Storing a list of apps is helpful not only for our research, but also because it allows us to further examine, via followup if necessary, any suspicious apps discovered during a consultation. In addition, whenever we update the blacklist, we retroactively scan the apps from past consultations to ensure that no newly found IPV spyware apps were on a previously scanned devices. (Fortunately, we have not yet detected any spyware retroactively.) All data is stored securely and accessible only to our team.

Detecting potential IPV spyware. A core feature of ISDi is its detection of IPV spyware apps (either overt or dual-use) on iOS or Android devices. To do so, ISDi integrates various heuristics into a rank-ordered list of apps by an internal threat score. After querying the device for a list of installed apps, ISDi assigns a threat score to each app, that score derived from summing the weights of heuristics.

The main heuristic is two blacklists of app IDs, one for overt spyware apps and one for dual-use apps. The blacklists deployed with ISDi was seeded with the list of apps discovered in [8], but then updated by using their snowball searching techniques on the Google Play store and iTunes store. Note that Google Play occasionally bans apps and reportedly banned some in response to the results of [8]. We do not remove apps from a blacklist should they be removed from the play store — they could have been downloaded and installed by an abuser before removal. We additionally included any apps we discovered via manual searches or that we discovered in any other way. Following [8], we aggressively added apps to a blacklist, at risk of creating false positives. This favors having a low false negative rate, and we built into our protocol the ability for consultants to handle false positives when they arose. To help with ordering, we kept a separate blacklist of overt spyware, with other apps appearing on the dual-use blacklist.

In addition to blacklists, ISDi uses a few other heuristics. First are regular expressions applied to application names, as described in Section 5. Second was that we marked any off-store app as potentially dangerous. Third was whether the device is a system app, meaning it was pre-installed on the device by the cellular provider or OS vendor.

We then gave a weighted score to each app according to the values shown in Figure 4. The score of an app is equal to the sum of the weights for the set of heuristics that apply to the app. A higher score denotes being potentially more dangerous. The weights are admittedly somewhat arbitrary, but roughly correspond to our perception of the danger each heuristic indicates. In practice, the number of apps on a device that were assigned risk signals by ISDi were sufficiently small that our choice of weights and rank-ordering did not make much of a difference during consultations.

App detection accuracy. While ISDi lists all apps on the device, and the consultant is encouraged to visually inspect

Heuristic	Weight	Description
Overt spyware blacklist	1.0	Known, overt spyware
Dual-use blacklist	0.8	Legitimate uses, but possibly harmful in certain situations
Offstore app	0.8	Not installed through an official app marketplace
Regex match	0.3	App name or ID contains 'spy', 'track', etc.
System app	-0.1	Pre-installed by device vendor

Figure 4: The ISDi heuristics for ordering apps. Each app is assigned a score that is the sum of the weights for each heuristic that applies to it.

the entire list, we would still consider it a false negative if a dangerous app was not flagged by one of the four heuristics (excluding the system app heuristic).

As discussed in Section 5, ISDi's accuracy depends in part on labor intensive web crawling and manual pruning. Our blacklist of dual-use apps included all 2,474 seed apps from Chatterjee et al. [8], as well as 3,263 new apps from our own periodic crawls since May 2018 and filtering using the ML classifier given in [8]. Unlike in [8], we do not manually prune the 3,263 apps we added to the blacklist to further remove apps falsely flagged by the machine learning classifier. During consultation, the consultant ignores apps that are not relevant, which was not a problem during our consultations.

Most overt spyware apps we have encountered (and certainly all dual-use apps we have inspected) do not try to hide their presence from a programmatic scan. However, for a few of the overt spyware apps we have observed that they chose innocuous-looking app IDs (such as "com.android.system"). This reiterates the need for programmatic scans, which are not fooled by this. However, if apps change their app IDs frequently to avoid detection, our blacklists may not cover the full set of app IDs associated with a spyware. We have observed that one overt offstore spyware app, mSpy, has published versions of its Android APK with different app IDs: sys.framework and core.framework, while others such as SpyToApp, FlexiSpy, and SpyZie have not changed their app IDs to our knowledge (we re-downloaded them in September 2018 and in February 2019). We have found no evidence that onstore dual-use apps change their app IDs, though Trackview has published their app twice on the Google Play Store, as both net.cybrook.trackview and app.cybrook.trackview under different developer IDs. We have added all of the changed app IDs to our blacklist as we have discovered them.

Finally we note that ISDi is not designed to detect more sophisticated malware, such as that used by national intelligence agencies. We believe such malware is unlikely to arise in IPV settings, since it requires special access to obtain it. For a client for which it is plausible that her abuser might have access to such capabilities (e.g., the abuser works as a computer security expert), a discussion about potential remediations, such as obtaining new devices, would be appropriate.

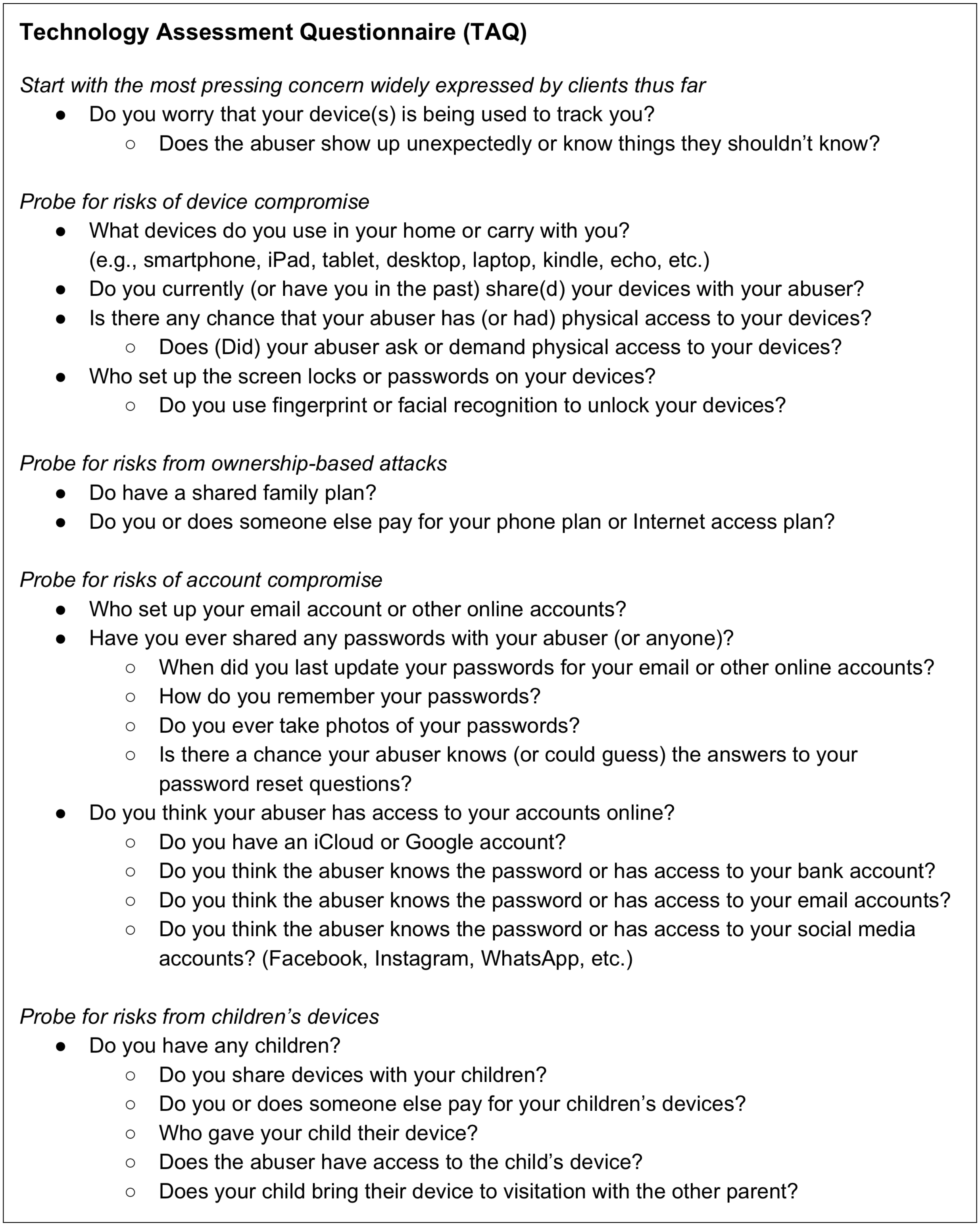
App reports. Upon clicking on an app, ISDi gives a number of details about the app. This includes a developer description (if available), when the app was installed (Android only), the permissions the app has requested, and the time of all the permissions recently used by the app (Android only), including dangerous permissions such as microphone, camera, or GPS. It also provides a link to a Google search on the app ID, which allows the consultant to quickly attempt to look up more information about the app should it be unfamiliar.

Detecting jailbroken or rooted phones. ISDi attempts to determine if the scanned device is jailbroken (iOS) or rooted (Android), since such devices are at much greater risk for installation of powerful spyware. For example, most spyware vendors enable for sophisticated features if the device is jailbroken/rooted. Moreover, it is unlikely that a client purposefully jailbreaks or roots their phone.

Thus ISDi uses a set of heuristics to determine whether a device is jailbroken/rooted. If any heuristic comes back positive, ISDi considers the device to be jailbroken or rooted and indicates this along with the results of the scan. Detecting jailbroken/rooted devices is under active discussion for both Android and iOS because app developer communities want to prevent their apps from being illegitimately being used on a jailbroken/rooted device. We therefore collected different heuristics from such community forums. For both iOS and Android, ISDi checks whether common jailbreak/rooting applications are installed on the device [3]. On Android devices, ISDi checks whether or not the su tool is installed on the system "shell" application [38]. On iOS devices, ISDi attempts to mount the filesystem at the root directory.

To the best of our understanding, ISDi will detect any jailbroken or rooted device. However, it is possible that a device could evade detection by ISDi using techniques that are not publicly known. We regularly look into app developer forums for new heuristics and update ISDi accordingly.

Possible attack vectors on ISDi. We have considered that spyware installed by an abuser on a client's phone may attempt to use its USB connection to ISDi as a possible attack vector [39, 41]. We are not aware of any overt spyware apps that try to misuse USB connections to a host computer. We ensured that all commands used by ISDi to communicate with iOS and Android devices, over libimobiledevice and adb, respectively, were run over least privilege (i.e., without sudo).



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?

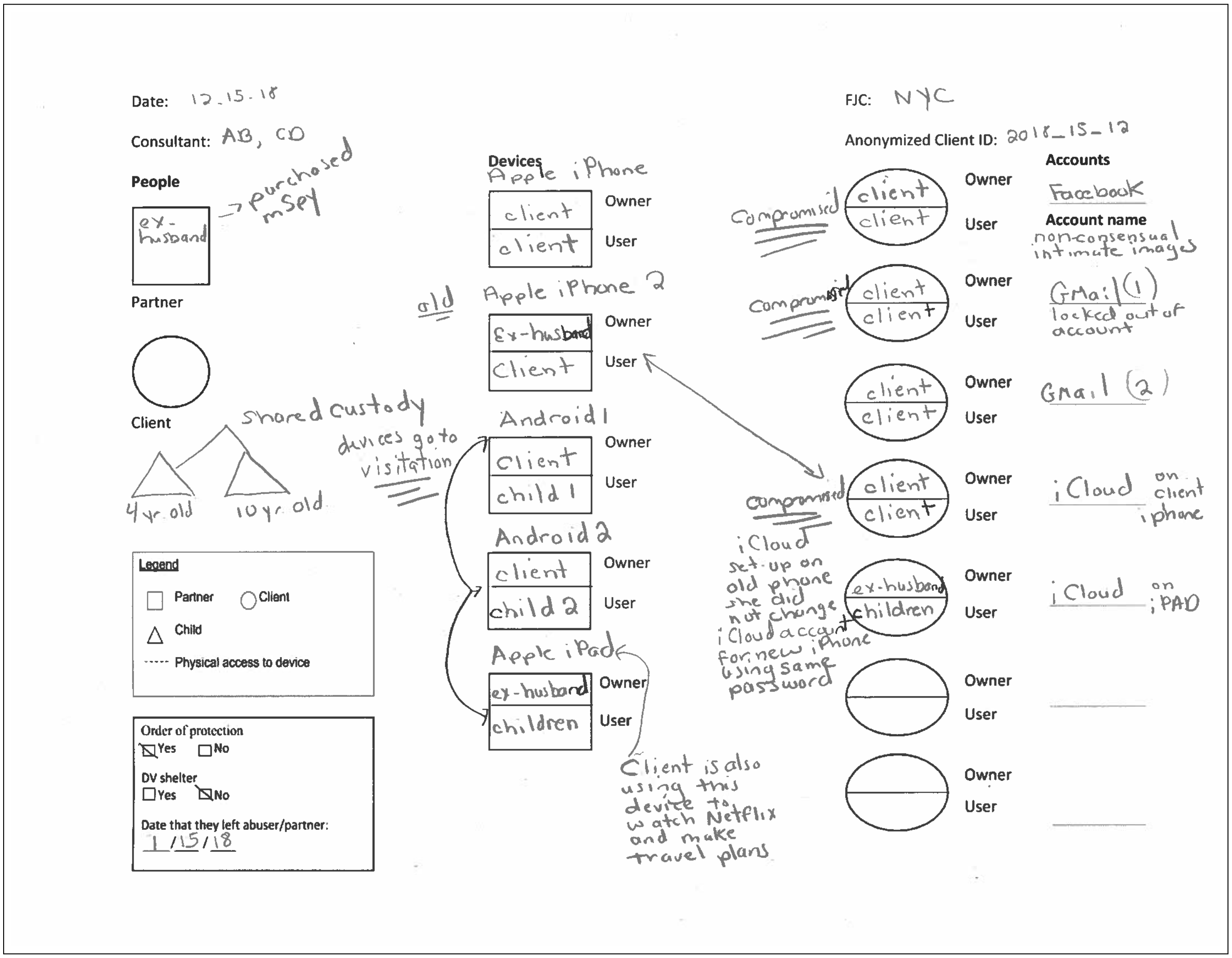
Probe for risks of account compromise

- 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?

Figure 5: The current version of the Technology Assessment Questionnaire (TAQ).



Date: 12.15.18

FJC: NYC

Consultant: AB, CD

Anonymized Client ID: 2018_15_12

People

ex-husband → purchased mSpy

Partner

Client

shared custody

4 yr. old

10 yr. old

devices go to visitation

Legend

□ Partner ○ Client

△ Child

----- Physical access to device

Order of protection

☒ Yes □ No

DV shelter

□ Yes ☒ No

Date that they left abuser/partner: 1 / 15 / 18

Devices

Apple iPhone

Owner: client

User: client

old Apple iPhone 2

Owner: ex-husband

User: Client

Android 1

Owner: client

User: child 1

Android 2

Owner: client

User: child 2

Apple iPad

Owner: ex-husband

User: children

Client is also using this device to watch Netflix and make travel plans

Accounts

compromised

Owner: client

User: client

Facebook

Account name

non-consensual intimate images

compromised

Owner: client

User: client

GMail (1)

locked out of account

Owner: client

User: client

GMail (2)

compromised

Owner: client

User: client

iCloud on client iphone

iCloud set-up on old phone she did not change iCloud account for new iPhone using same password

Owner: ex-husband

User: children

iCloud on iPAD

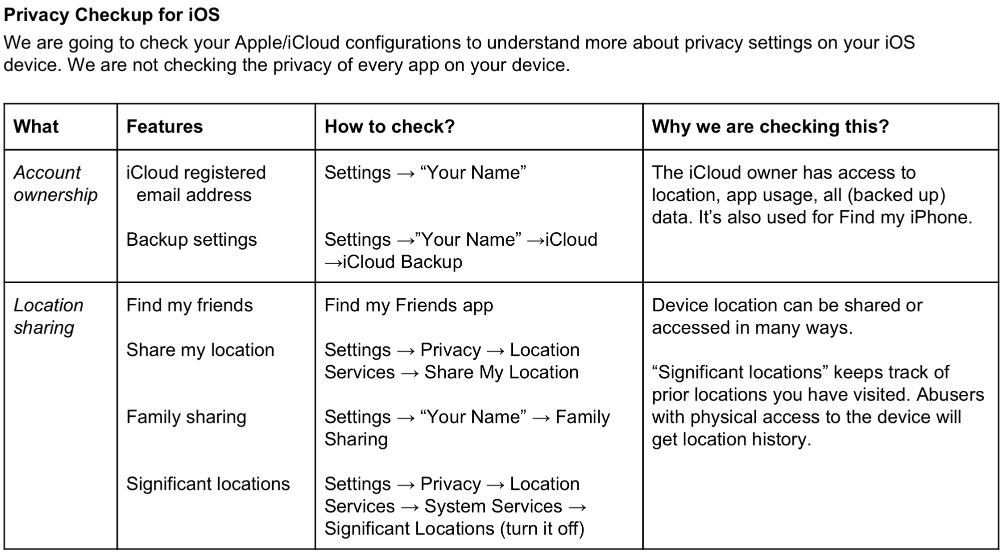
Owner

User

Owner

User

Figure 6: An example technograph as it might have been filled out for Carol's hypothetical scenario (described in Section 2).

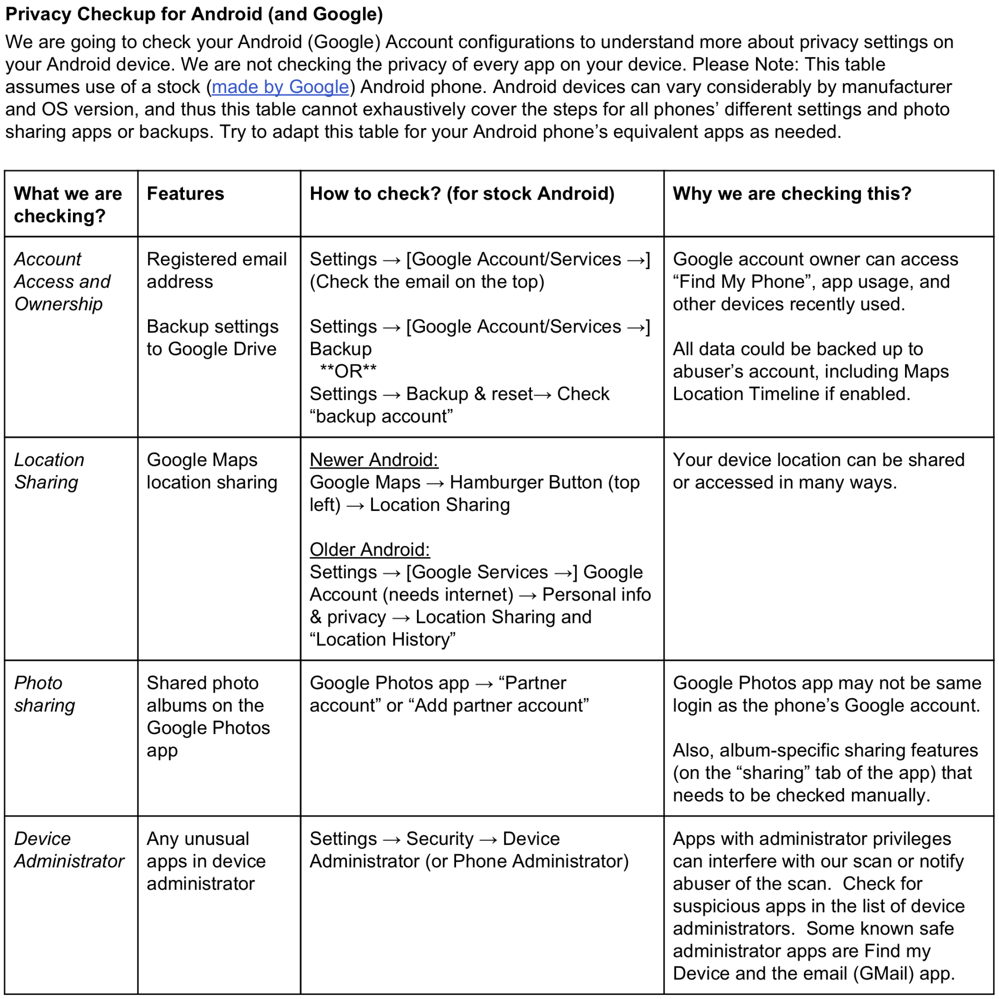


Privacy Checkup for iOS

We are going to check your Apple/iCloud configurations to understand more about privacy settings on your iOS device. We are not checking the privacy of every app on your device.

What	Features	How to check?	Why we are checking this?
Account ownership	iCloud registered email address Backup settings	Settings → “Your Name” Settings →”Your Name” →iCloud →iCloud Backup	The iCloud owner has access to location, app usage, all (backed up) data. It’s also used for Find my iPhone.
Location sharing	Find my friends Share my location Family sharing Significant locations	Find my Friends app Settings → Privacy → Location Services → Share My Location Settings → “Your Name” → Family Sharing Settings → Privacy → Location Services → System Services → Significant Locations (turn it off)	Device location can be shared or accessed in many ways. “Significant locations” keeps track of prior locations you have visited. Abusers with physical access to the device will get location history.

Figure 7: Protocol for manually checking a client’s iOS privacy settings.

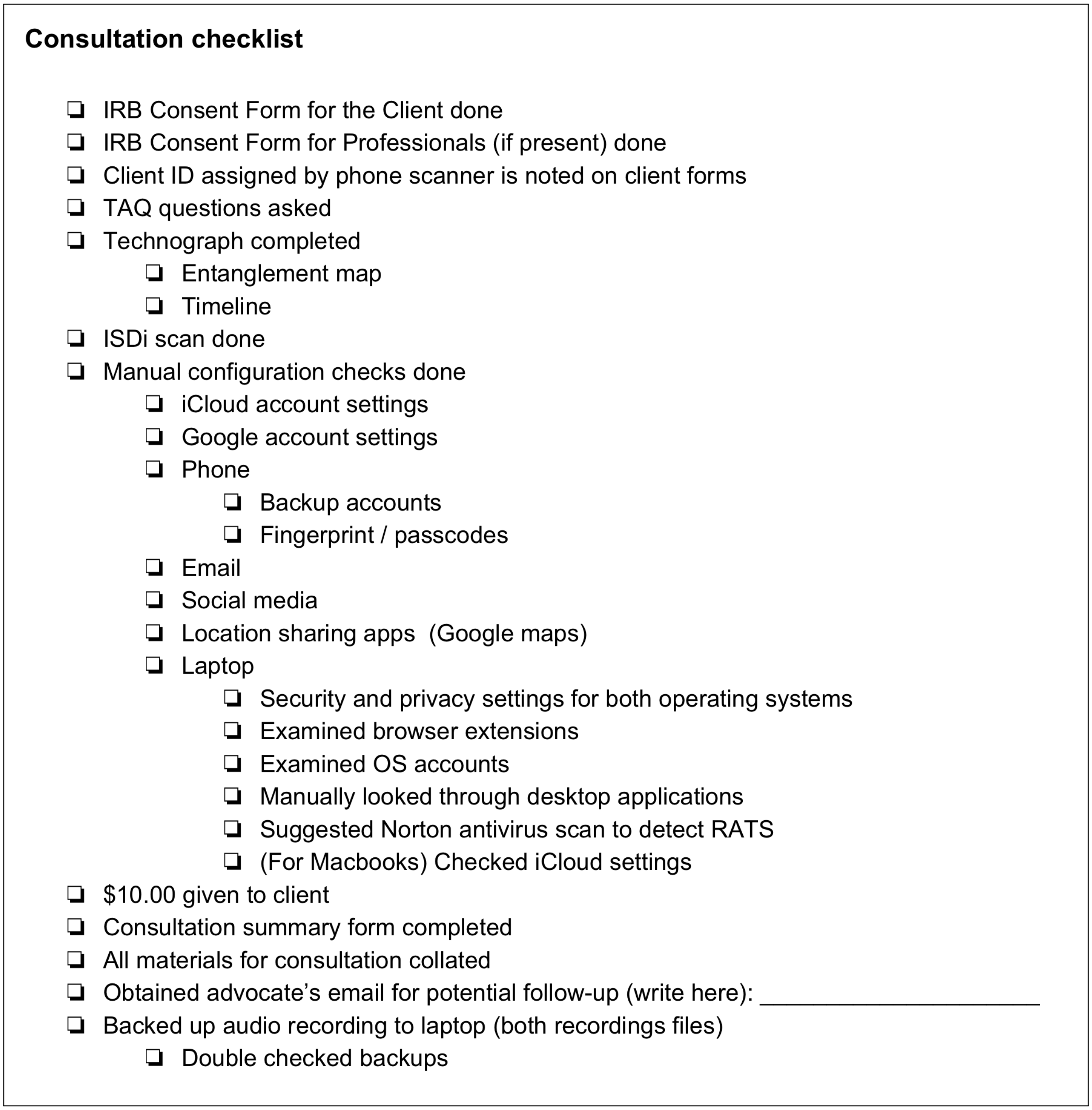


Privacy Checkup for Android (and Google)

We are going to check your Android (Google) Account configurations to understand more about privacy settings on your Android device. We are not checking the privacy of every app on your device. Please Note: This table assumes use of a stock (made by Google) Android phone. Android devices can vary considerably by manufacturer and OS version, and thus this table cannot exhaustively cover the steps for all phones’ different settings and photo sharing apps or backups. Try to adapt this table for your Android phone’s equivalent apps as needed.

What we are checking?	Features	How to check? (for stock Android)	Why we are checking this?
Account Access and Ownership	Registered email address Backup settings to Google Drive	Settings → [Google Account/Services →] (Check the email on the top) Settings → [Google Account/Services →] Backup **OR** Settings → Backup & reset→ Check “backup account”	Google account owner can access “Find My Phone”, app usage, and other devices recently used. All data could be backed up to abuser’s account, including Maps Location Timeline if enabled.
Location Sharing	Google Maps location sharing	Newer Android: Google Maps → Hamburger Button (top left) → Location Sharing Older Android: Settings → [Google Services →] Google Account (needs internet) → Personal info & privacy → Location Sharing and “Location History”	Your device location can be shared or accessed in many ways.
Photo sharing	Shared photo albums on the Google Photos app	Google Photos app → “Partner account” or “Add partner account”	Google Photos app may not be same login as the phone’s Google account. Also, album-specific sharing features (on the “sharing” tab of the app) that needs to be checked manually.
Device Administrator	Any unusual apps in device administrator	Settings → Security → Device Administrator (or Phone Administrator)	Apps with administrator privileges can interfere with our scan or notify abuser of the scan. Check for suspicious apps in the list of device administrators. Some known safe administrator apps are Find my Device and the email (GMail) app.

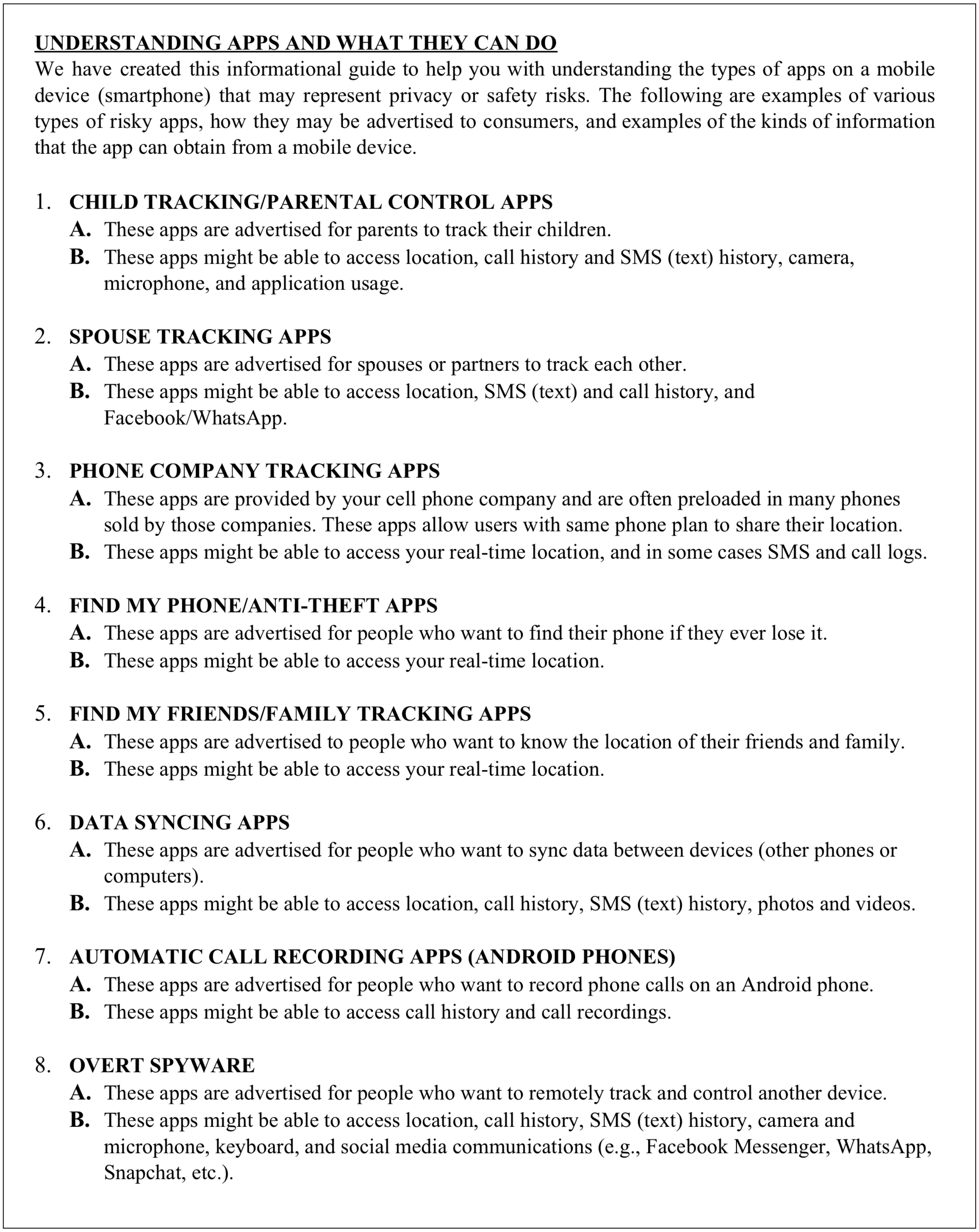
Figure 8: Protocol for manually checking a client’s Google and Android privacy settings.



Consultation checklist

- □ IRB Consent Form for the Client done
- □ IRB Consent Form for Professionals (if present) done
- □ Client ID assigned by phone scanner is noted on client forms
- □ TAQ questions asked
- □ Technograph completed
    - □ Entanglement map
    - □ Timeline
- □ ISDi scan done
- □ Manual configuration checks done
    - □ iCloud account settings
    - □ Google account settings
    - □ Phone
        - □ Backup accounts
        - □ Fingerprint / passcodes
    - □ Email
    - □ Social media
    - □ Location sharing apps (Google maps)
    - □ Laptop
        - □ Security and privacy settings for both operating systems
        - □ Examined browser extensions
        - □ Examined OS accounts
        - □ Manually looked through desktop applications
        - □ Suggested Norton antivirus scan to detect RATS
        - □ (For Macbooks) Checked iCloud settings
- □ $10.00 given to client
- □ Consultation summary form completed
- □ All materials for consultation collated
- □ Obtained advocate’s email for potential follow-up (write here): ______________________
- □ Backed up audio recording to laptop (both recordings files)
    - □ Double checked backups

Figure 9: Checklist that is completed by the tech consultant during and after each client consultation.



UNDERSTANDING APPS AND WHAT THEY CAN DO

We have created this informational guide to help you with understanding the types of apps on a mobile device (smartphone) that may represent privacy or safety risks. The following are examples of various types of risky apps, how they may be advertised to consumers, and examples of the kinds of information that the app can obtain from a mobile device.

1. **CHILD TRACKING/PARENTAL CONTROL APPS**
   A. These apps are advertised for parents to track their children.
   B. These apps might be able to access location, call history and SMS (text) history, camera, microphone, and application usage.

2. **SPOUSE TRACKING APPS**
   A. These apps are advertised for spouses or partners to track each other.
   B. These apps might be able to access location, SMS (text) and call history, and Facebook/WhatsApp.

3. **PHONE COMPANY TRACKING APPS**
   A. These apps are provided by your cell phone company and are often preloaded in many phones sold by those companies. These apps allow users with same phone plan to share their location.
   B. These apps might be able to access your real-time location, and in some cases SMS and call logs.

4. **FIND MY PHONE/ANTI-THEFT APPS**
   A. These apps are advertised for people who want to find their phone if they ever lose it.
   B. These apps might be able to access your real-time location.

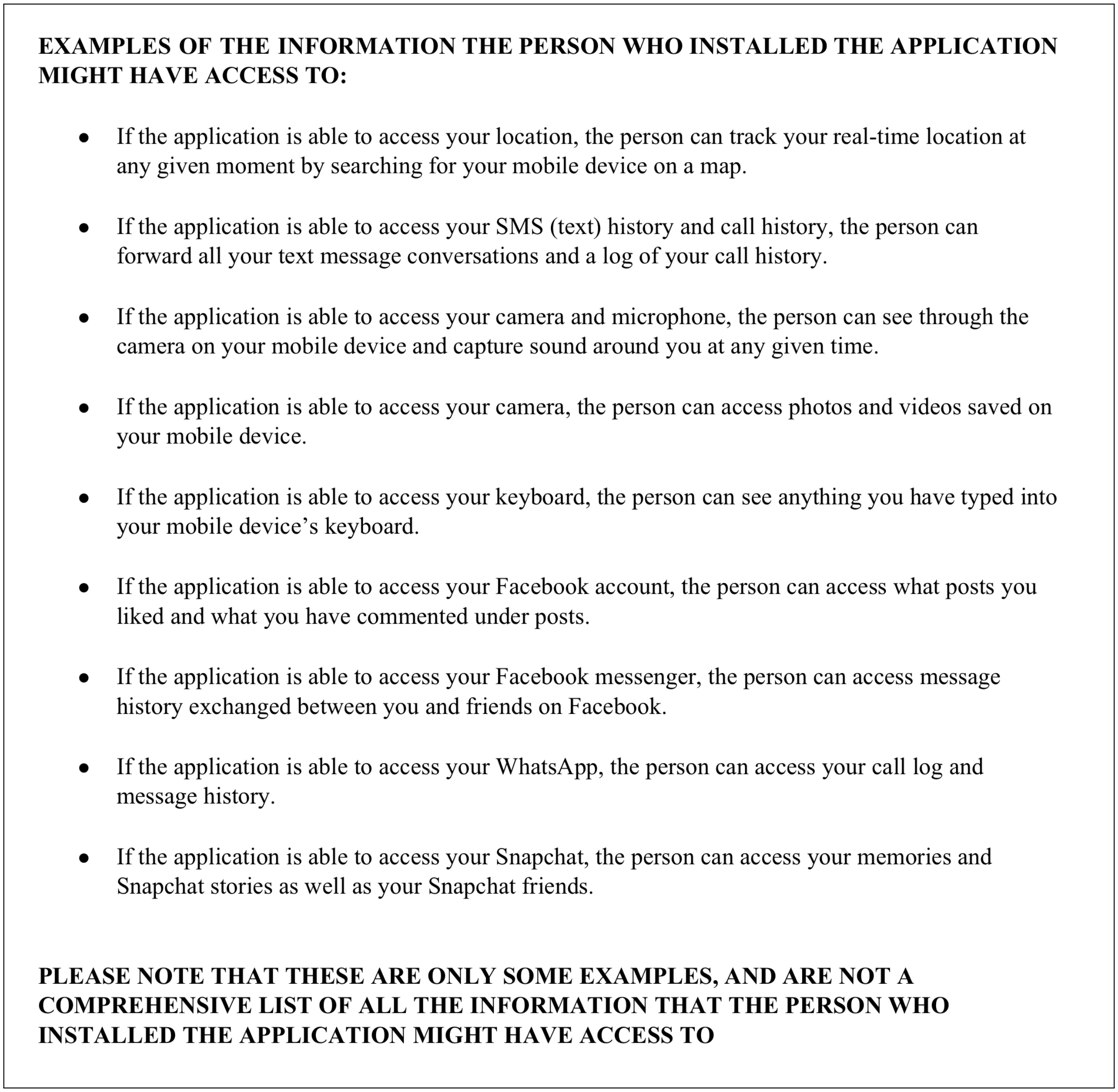
5. **FIND MY FRIENDS/FAMILY TRACKING APPS**
   A. These apps are advertised to people who want to know the location of their friends and family.
   B. These apps might be able to access your real-time location.

6. **DATA SYNCING APPS**
   A. These apps are advertised for people who want to sync data between devices (other phones or computers).
   B. These apps might be able to access location, call history, SMS (text) history, photos and videos.

7. **AUTOMATIC CALL RECORDING APPS (ANDROID PHONES)**
   A. These apps are advertised for people who want to record phone calls on an Android phone.
   B. These apps might be able to access call history and call recordings.

8. **OVERT SPYWARE**
   A. These apps are advertised for people who want to remotely track and control another device.
   B. These apps might be able to access location, call history, SMS (text) history, camera and microphone, keyboard, and social media communications (e.g., Facebook Messenger, WhatsApp, Snapchat, etc.).

Figure 10: Part 1 of the app classification guide that we offered to clients when we scanned their devices using ISDi.

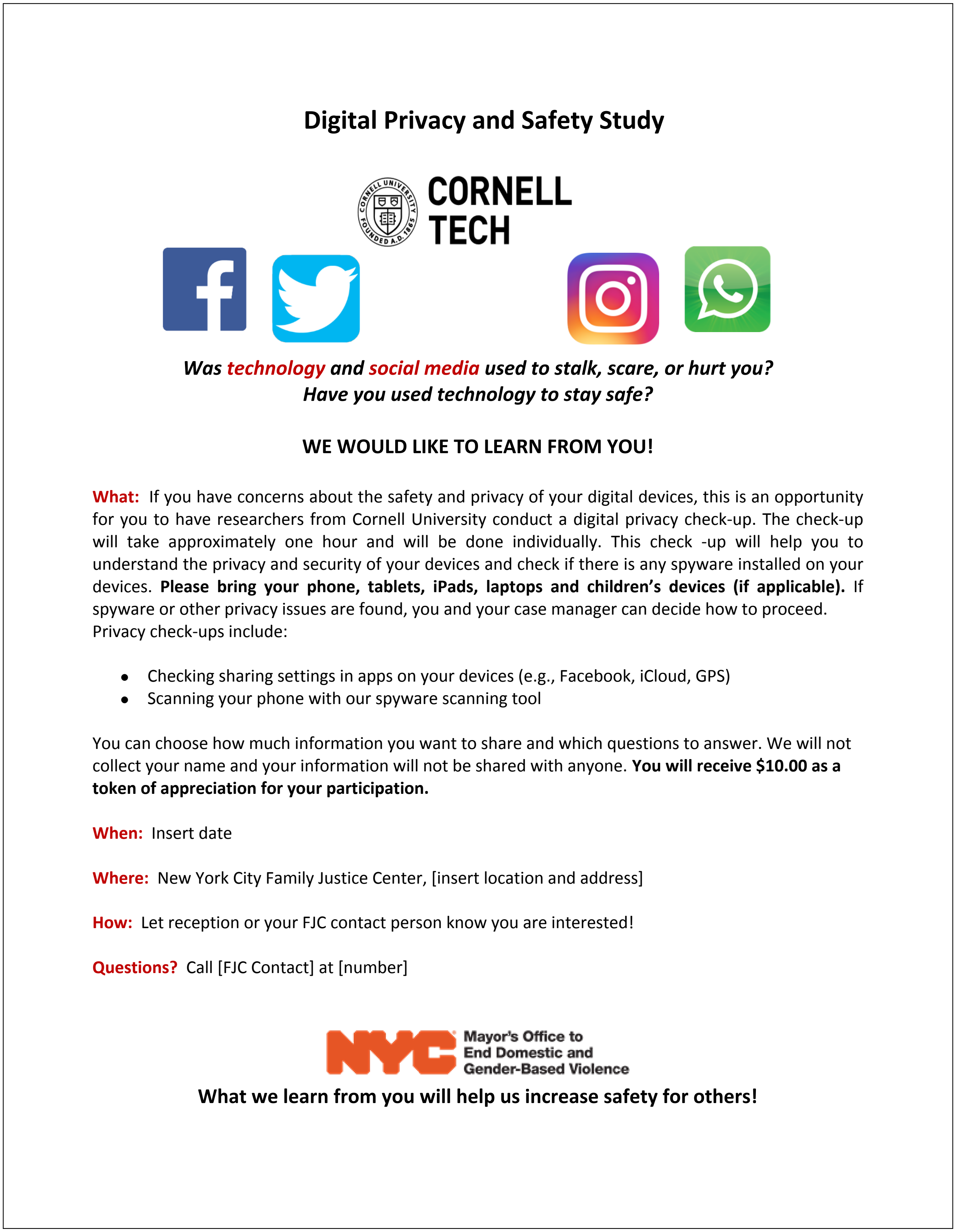


EXAMPLES OF THE INFORMATION THE PERSON WHO INSTALLED THE APPLICATION MIGHT HAVE ACCESS TO:

- If the application is able to access your location, the person can track your real-time location at any given moment by searching for your mobile device on a map.
- If the application is able to access your SMS (text) history and call history, the person can forward all your text message conversations and a log of your call history.
- If the application is able to access your camera and microphone, the person can see through the camera on your mobile device and capture sound around you at any given time.
- If the application is able to access your camera, the person can access photos and videos saved on your mobile device.
- If the application is able to access your keyboard, the person can see anything you have typed into your mobile device’s keyboard.
- If the application is able to access your Facebook account, the person can access what posts you liked and what you have commented under posts.
- If the application is able to access your Facebook messenger, the person can access message history exchanged between you and friends on Facebook.
- If the application is able to access your WhatsApp, the person can access your call log and message history.
- If the application is able to access your Snapchat, the person can access your memories and Snapchat stories as well as your Snapchat friends.

PLEASE NOTE THAT THESE ARE ONLY SOME EXAMPLES, AND ARE NOT A COMPREHENSIVE LIST OF ALL THE INFORMATION THAT THE PERSON WHO INSTALLED THE APPLICATION MIGHT HAVE ACCESS TO

Figure 11: Part 2 of the app classification guide that we offered to clients when we scanned their devices using ISDi.



Digital Privacy and Safety Study

CORNELL TECH

Was technology and social media used to stalk, scare, or hurt you?
Have you used technology to stay safe?

WE WOULD LIKE TO LEARN FROM YOU!

What: If you have concerns about the safety and privacy of your digital devices, this is an opportunity for you to have researchers from Cornell University conduct a digital privacy check-up. The check-up will take approximately one hour and will be done individually. This check -up will help you to understand the privacy and security of your devices and check if there is any spyware installed on your devices. **Please bring your phone, tablets, iPads, laptops and children's devices (if applicable).** If spyware or other privacy issues are found, you and your case manager can decide how to proceed. Privacy check-ups include:

- Checking sharing settings in apps on your devices (e.g., Facebook, iCloud, GPS)
- Scanning your phone with our spyware scanning tool

You can choose how much information you want to share and which questions to answer. We will not collect your name and your information will not be shared with anyone. **You will receive $10.00 as a token of appreciation for your participation.**

When: Insert date

Where: New York City Family Justice Center, [insert location and address]

How: Let reception or your FJC contact person know you are interested!

Questions? Call [FJC Contact] at [number]

NYC Mayor's Office to End Domestic and Gender-Based Violence

What we learn from you will help us increase safety for others!

Figure 12: The flier we used for recruiting study participants.