A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19

Emily Tseng
Cornell University
New York, NY, USA
et397@cornell.edu

Diana Freed
Cornell University
New York, NY, USA
dlf92@cornell.edu

Kristen Engel
Jacobs Institute, Cornell Tech
New York, NY, USA
ke242@cornell.edu

Thomas Ristenpart
Cornell Tech
New York, NY, USA
ristenpart@cornell.edu

Nicola Dell
Jacobs Institute, Cornell Tech
New York, NY, USA
nixdell@cornell.edu

ABSTRACT

The shutdown measures necessary to stop the spread of COVID-19 have amplified the role of technology in intimate partner violence (IPV). Survivors may be forced to endure lockdowns with their abusers, intensifying the dangers of technology-enabled abuse (e.g. stalking, harassment, monitoring, surveillance). They may also be forced to rely on potentially compromised devices to reach support networks: a dangerous dilemma for digital safety. This qualitative study examines how technologists with computer security expertise provided remote assistance to IPV survivors during the pandemic. Findings from 24 consults with survivors and five focus groups with technologist consultants show how remote delivery of technology support services raised three fundamental challenges: (1) ensuring safety for survivors and consultants; (2) assessing device security over a remote connection; and (3) navigating new burdens for consultants, including emotional labor. We highlight implications for HCI researchers creating systems that enable access to remote expert services for vulnerable people.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Social aspects of security and privacy.*

KEYWORDS

intimate partner violence, gender-based violence, computer security and privacy

ACM Reference Format:
Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3411764.3445589

1 INTRODUCTION

As digital technologies become more and more embedded in modern life, it becomes ever more imperative for people to safeguard the security and privacy of their devices and digital assets. Protecting oneself against threats like surveillance, harassment, and doxxing requires not just technical knowledge of potential vulnerabilities, but also the wherewithal to mount and maintain the right defenses: Built-in security mechanisms often fail in the face of targeted and persistent attacks [15, 31, 46]. These attacks are particularly pronounced in the context of intimate partner violence (IPV), defined as violence enacted against a person by a current or former intimate partner (e.g. a spouse or significant other). When intimate partners become abusers, their access to and knowledge of their victims' lives can render common computer security and privacy systems ineffective [49]. Indeed, a growing body of work has documented the many ways abusers exploit digital technologies to track, monitor, harass, and control their victims [14, 37, 38, 51, 75].

To better support IPV survivors, advocates have advanced a number of interventions: notably, programs connecting survivors directly with technologists who have computer security expertise, such as the technology-enabled coercive control (TECC) clinic in Seattle [26] and Operation Safe Escape [30]. Havron et al. [44] called such approaches *clinical computer security*, and proposed a framework for in-person consultations in which a technologist with computer security expertise (the *consultant*) meets face-to-face with a survivor (the *client*) in a secure location, to understand their situation, investigate possible vulnerabilities, and advise on mitigation strategies. Early evidence suggests that clinical computer security interventions are helpful and rapidly becoming a key facet of survivor support [36, 44].

The recent shutdowns necessary to stop the spread of COVID-19 have threatened to completely derail survivor support systems. Face-to-face meetings were prohibited just as cases of domestic violence increased globally [72, 79, 85], and all kinds of support services have had to rapidly transition to remote delivery even as many survivors have to endure lockdown orders with their abusers. Amid mounting evidence suggesting victims are finding

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445589

it harder and harder to seek help [70], access to safe and private digital communications has become paramount for clients and support workers alike. But without prior research on how to safely provide remote computer security support to survivors, these clinics have to quickly design and deploy new protocols. All this begs the questions of whether these deployed efforts are effective and, more broadly, what best practice should be for remotely delivered computer security assistance for IPV survivors. Answers to these questions would be applicable beyond the COVID-19 context, for the expansion of access to support services to anyone limited by geography, socioeconomic or ability status, or personal preference.

We therefore initiate study of remote delivery of computer security assistance for IPV survivors via an in-depth reflexive examination of a computer security clinic in New York City. The Clinic to End Tech Abuse (CETA)[1], in which each author volunteers, served clients via face-to-face consults before the COVID-19 pandemic. When state-mandated lockdowns began in March 2020, CETA needed to transition service, with little interruption, in what was at the time the global epicenter of the pandemic. This required designing new protocols for everything from appointment scheduling and team debriefings to spyware checks and safety planning. We studied the challenges faced in remote delivery, and how they compared to those encountered in in-person consults, via qualitative analysis of data from 24 remote consults with survivors that took place between March and August of 2020, as well as five reflective focus groups conducted with seven consultants who had experience with remote and in-person contexts. Our reflective and reflexive methodology (detailed in Section 4) enabled us to delve deep into what were at times emotionally charged topics.

Our findings highlight the fundamental challenges faced in providing tech abuse services remotely. First, we found consultants struggled with how to assess clients' safety in advance of an appointment, and how to maintain it throughout the consult (Section 5.1). Maintaining privacy on each call was important to consultants, given that both parties were often communicating from inside their homes; but in practice, clients often could not guarantee they were calling from a location or device to which the abuser had never had access. Relatedly, we found the remote context presented particular challenges for consultants' ability to investigate clients' devices for compromise (Section 5.2). Safety procedures dictated clients and consultants should communicate over audio only, requiring consultants to find new ways to navigate clients' devices and accounts; but these measures created such substantial inefficiencies that consultants began to rely on follow-up emails to conduct full investigations. Lastly, we found the remote context created substantial new burdens for consultants, including increases to the volume of work required of each consult, the mental overhead of switching in and out of consults amidst other tasks, and the emotional labor necessary for the work (Section 5.3).

Drawing on these findings, we highlight three key tradeoffs in the provision of any expert service over a computer-mediated connection, and recommendations for addressing each (Section 6). Where balancing safety and efficiency is concerned, we argue that consultative services should support a plurality of communication modalities and safety measures, rather than a one-size-fits-all policy. Tailored services would, for example, enable consultants and clients who wanted to connect over video to enjoy the benefits of visual cues. We also propose that consultative services work to better understand the many forms of emotional labor required in remote services, and adopt structures that recognize and support this often-invisible work. Finally, we argue that these services should consider how their advice may enable clients to develop their own capacities where digital security is concerned—or create new unwanted burdens.

Our study extends the growing body of work within HCI examining how computer security experts can support survivors of tech abuse in IPV [36, 44]. We additionally contribute to the literature on remote provision of expert services more broadly (e.g. in medicine [35, 63, 80] and education [2, 5, 48]), as well as discourse on how technology can support the needs of vulnerable and marginalized people [18, 22, 28, 29].

2 RELATED WORK

Support services for victims of IPV are the subject of substantial prior research. Drawing on growing evidence that the COVID-19 pandemic may have exacerbated the incidence of IPV worldwide [53], a 2020 United Nations report called domestic violence during COVID-19 "the shadow pandemic" [83]. The urgency of addressing IPV under COVID has renewed researchers' calls for public health approaches to IPV as a form of gender-based violence that disproportionately impacts women and children [13]. Researchers have advanced that these approaches should foreground intersectional approaches to trauma-informed care by tailoring services to victims' particular circumstances and identities [47]. In parallel, prior work has examined the emotional labor required when providing and conducting research in trauma-informed care for IPV [12, 17].

Our work contributes to this literature with a study of one particular type of victim support service—one focused on technology-related abuse—in the context of pandemic-related shutdowns in a major urban center in the U.S. We begin this section by situating our study within the prior literature on tech-focused victim support services. We then discuss prior work on the provision of consultative services via remote communication tools.

Supporting survivors of tech-enabled IPV. A growing body of research documents how abusers use technology to extend and amplify IPV, including access-based attacks by a UI-bound adversary (one who uses standard interfaces), remote attacks through sensitive information disclosure and unsolicited contact, and the use of common apps repurposed as spyware (so-called dual-use apps) [14, 21, 38, 65, 84]. In parallel, research has shown a bevy of resources online provide instructions on how to enact tech abuse, including blogs, videos, and online forums [14]. Most recently, Tseng et al. [75] showed that abusers learn targeted strategies for intimate partner surveillance within online forums dedicated to discussions of infidelity. The threat of tech abuse persists even as survivors leave their abuser's physical control and establish a life apart [21, 51, 84]. Further, even in the absence of observed attacks, the perception of the threat impacts survivors' usage and trust in technology, often causing further isolation from resources and support networks [50].

[1] https://www.ceta.tech.cornell.edu/

In the face of these threats, IPV survivor advocates, technology companies, and academics are examining how to assist clients with tech abuse. Research has shown that commercial tech support services, like Geek Squad [66] or Apple Support [3], are often not sufficiently tailored to the safety and security needs of IPV survivors [37]. Resources that more closely consider survivors' needs are offered by organizations such as the National Network to End Domestic Violence's Safety Net Project [74] and Coalition Against Stalkerware [67], and advocates and academics have also created apps to help survivors navigate and document tech abuse [9, 73, 81]. However, it can be challenging for survivors and professionals to know how to act on this advice [37]. Other groups have developed interventions that provide personalized in-person and/or face-to-face assistance to specific individuals experiencing tech abuse. For example, the technology-enabled coercive control (TECC) clinic was recently established to help survivors experiencing tech abuse in Seattle [26], and Operation: Safe Escape offers computer security assistance to survivor services and advocates [30]. Havron et al. [44] describe this approach as *clinical computer security*, in which a trained technologist provides a face-to-face consultation to a client (the term used for IPV survivors seeking help via support services) [36]. Other groups have developed similar approaches for people experiencing tech abuse in contexts outside of IPV, including the Citizen Lab [20] and Citizen Clinic [34], which help people facing digital attacks by nation-states, and ad hoc help provided by computer security experts to individuals suffering attacks [45].

These support systems have, of course, been affected by the ongoing COVID-19 pandemic. Recent work indicates the public health measures implemented to combat COVID-19 have exacerbated abusive conditions and reduced survivors' access to support, leading to a global increase in reports of domestic violence [11, 53, 79, 85]. Effects of the pandemic are constraining budgets and staffing at a time when services need to transition online, adding to the burdens on service providers, who must find safe ways to remotely connect to their clients [72, 85]. Advocates are also pursuing digital strategies to expand public awareness of IPV, and to extend the reach of resources so that marginalized groups are not left behind [25, 78]. As the pandemic evolves, researchers and practitioners in IPV support continue to grapple with how to balance expanding the reach of support services against the risks of providing support in less-controlled environments. In this work, we study these tensions by examining one real-world deployment of a clinical computer security intervention for survivors of tech abuse.

Remote consultative services. Given the need for support services to move to remote service delivery, a relevant line of prior work studies communication technologies that support the provision of expert services to people whose physical location, socioeconomic or ability status, or personal preferences prevent them from accessing help in-person. The role of technology in expanding access to vital consult services has been studied extensively in domains such as mental health [7, 80], legal advice [52], and education [2, 5, 48]. Crabtree et al. note that across domains, "help-giving" can be seen to require extensive *articulation work*, in which seeker and provider engage in an ongoing discussion collaboratively specifying problems and elaborating potential solutions [19].

However, research on remote interactions has shown that connection quality and consistency universally impact users' experience with and trust in collaborative technology-mediated interactions [16]. At issue is the degradation of the interpersonal connection: Establishing rapport via nonverbal communication can be integral to effective consultation interventions, increasing trust and client buy-in [71], but in a remote communication environment, both client and consultant lack social presence and non-verbal cues, making it more difficult to build rapport. Prior work on remote communication has shown this can lead to greater uncertainty in both the client and consultant [57, 59], feelings of isolation [77], and communication misunderstandings [57].

The success of a shift in service modalities can also hinge on providers' acceptance of the burdens associated with computer-mediated communication. Beyond adapting to the inherent challenges of remote communication, issues may arise with the integration of a care methodology—which itself must be adapted for the context—with remote interaction with the client [63]. At issue is the provider's diminished *control* over the consultation environment: The absence of physical access can undermine the consultant's ability to ensure client privacy [5, 7, 53] and effective recourse in the event of escalation into crisis [7]. Indeed, prior work on the provision of mental health and education services remotely show that remote delivery places a greater, yet less visible burden on service providers [58, 61].

Prior work has examined how to best compensate for the issues that arise from remote service provision outside IPV contexts. A number of these mitigation strategies suggest adaptations within the client-consultant relationship to establish trust in the absence of in-person interactions, including the use of reinforcement and self-disclosure to elicit reciprocity [60]. These adaptations must also account for differing levels of technology literacy: Gautam et al.'s research demonstrates the importance of tailoring remote communication to the client to increase understanding, e.g. by conveying instructions using the client's colloquialisms and preparing metaphors and explanations for technical jargon [41]. Outside of adjustments to communication styles, prior work has also suggested adapting the modality itself, e.g. through the use of wide-frame video [55] or additional lines of connection [1]. In practice, service providers must also consider carefully the vendor from which they procure their communication tools: prior work notes the profit motives in commercial technology are at times in conflict with client interests, especially with regard to privacy [43].

Our work builds on this literature by contributing a reflective and reflexive qualitative study that examines how these difficulties manifest in a uniquely fraught context: the provision of remote support services for survivors of tech-enabled IPV. This context presents a unique complication of the remote service paradigm: often, clients must communicate with consultants on the very devices they suspect an abuser might be surveilling. We examine new and existing mitigation strategies in this environment for assessing and ensuring participant safety and conducting investigations.

3 RESEARCH CONTEXT

Before describing our study methods in detail, we first provide essential background on the computer security clinic for IPV survivors (tech clinic hereafter) within which our study took place.

The Clinic to End Tech Abuse (CETA) was established in October 2018 in partnership with the New York City (NYC) Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV) [27]. CETA's goal is to provide IPV survivors with appropriate technology assistance and safety planning that is personalized to their specific context. At the time of our study, with the exception of a full-time Director, the clinic was staffed entirely by volunteers: primarily graduate students and faculty in computer and information science, as well as other professionals with technical expertise. All staff completed a series of training workshops on trauma-informed care and on the sociotechnical aspects of tech-enabled IPV.

Prior to March 2020, CETA offered in-person consults to individual clients (the term used for IPV survivors in this context) from within NYC's Family Justice Center system (FJCs) [33]. Clients were referred by an IPV professional (e.g., social worker, lawyer) on their case. Sixty-minute in-person consults were then held at FJCs by trained technologist consultants, who typically worked in pairs (two consultants per appointment).

Consults followed an understand-investigate-advise (UIA) framework (adapted from Havron et al. [44]) that began with a semi-structured interview to *understand* the client's situation, including their digital footprint (devices and accounts they use) and any entanglements (other devices, accounts, or people who may impact their computer security). The *investigation* part of a consult then involved programmatic scanning of devices for spyware using a custom-built tool and manual investigation of devices and online accounts for evidence of problems or potential insecurities, such as recent logins from devices known to belong to the abuser, family sharing configurations that could leak data, or evidence of vulnerable accounts due to poor password selection and lack of two-factor authentication. Finally, the consultants worked with both the referring IPV professional and the client to provide *advice* about how clients might mitigate technology issues. Importantly, this involved appropriate safety planning to avoid potential escalation of the abuse that might result from changes the client made to their technology. From October 2018 to March 2020, CETA delivered in-person consults to 144 clients in all five boroughs of NYC. The last in-person consult took place on March 12, 2020.

As COVID-19 cases and deaths rose dramatically in NYC in March 2020, a large number of survivor support services closed their physical offices indefinitely—including the FJCs. Thus, to continue to serve clients, CETA quickly created a protocol for remote-only client services delivered via password-protected, audio-only conference calls. After rapid development of this protocol, the first remote consult took place on March 27, 2020.

In the remote service model, clients continue to be referred to CETA by IPV professionals, who are also operating remotely. To protect confidentiality, all communication regarding an appointment is routed through the IPV professional, such that the client remains anonymous to clinic volunteers. Consultants coordinate with the referring IPV professional via secure email to make an appointment for the client. The IPV professional also completes an intake form that provides basic details of the client's case, including whether the client has access to a safe *location* and a safe *device* (one to which their abuser has not had physical access) from which to call in for the consult. (We discuss safety challenges more in Section 5.1). Through back-and-forth communication with the IPV professional, clinic volunteers then establish a mutually agreeable date and time for the consult, which the IPV professional shares with the client along with password-protected dial-in information.

Remote consults are scheduled for 60 minutes, and attended by the client and two trained consultants. Once both parties have joined the audio-only conference line, consultants begin by confirming that the client is connecting from a safe location and on a safe device, before walking the client through informed consent procedures. The consult then follows a modified version of the UIA framework. Although the semi-structured interview to understand the client's situation is relatively similar to in-person consults, the investigations of the client's technology is very different. The remote setting means that consultants are unable to connect the client's devices to a laptop to scan for spyware. Instead, all investigations proceed manually, with a consultant verbally providing step-by-step instructions to the client, who follows the instructions to check the security and privacy of their accounts and concerning apps. (We discuss further the challenges around remote navigation of clients' devices in Section 5.2). Finally, the consultants and client discuss potential vulnerabilities discovered during the session. The consultants inform the client of potential consequences of taking actions, and advise the client to safety plan with their referring IPV professional before making any changes.

Between March and September 2020, CETA provided 32 remote consults to clients, 24 of which are in our dataset. CETA continues to offer remote services to clients in NYC at the time of writing.

4 METHODS

The goal of our study was to examine how the push to remote-only interaction required by the COVID-19 pandemic impacted the delivery of computer security support to IPV survivors. To accomplish this, we studied data from (1) real-world remote consults, and (2) reflective focus groups with the consultants who delivered them. Together, these data illuminate the dynamics of client-consultant interactions during remote consults, as well as consultants' reflections on how remote service delivery compared to their experiences with in-person consults. All study procedures were approved by our institutional IRB.

Reflection, reflexivity, and positionality. Given the nature of our work, it is essential to disclose that each of the five authors of this paper volunteers in CETA, where they are members of a larger team of 20+ people. Some of the authors' experiences are represented in our consult data, and all but one author participated in at least one focus group (discussed below). As a result, some of our personal biases and experiences are included in our findings, and thus our methods should be understood as *reflective* and *reflexive* forms of qualitative research [62, 64].

Employing a reflexive methodology enabled us to probe into sensitive issues by creating *interactive interview* environments. In our focus groups, we cultivated collaborative sensemaking between people in the role of the researchers and people in the role of participants [24]. In creating a site for collaborative reflection and rotating researchers between subjectivity and objectivity, we were able to achieve a robust understanding of the emotionally charged topics at hand.

In addition to employing reflexivity in our data collection, we engaged continually in reflexive methodologies throughout analysis. Prior work has advanced the reflexive approach as one that allows the researcher to move outside of the research process and critically reflect by cultivating self-awareness of the process—an essential component of ethical research [39, 64]. Throughout the analysis and writing of this paper, we adopted a reflexive approach to ensure that our opinions and biases were presented critically.

Data collection. Our data consist of (1) notes and recordings from 24 consults with clients, and (2) transcripts of five focus groups with seven technologist consultants. Due to restrictions on in-person meetings during the COVID-19 pandemic, all client consults and consultant focus groups took place via audio-only conference calls, and all participants provided verbal consent to participate in our IRB-approved research.

Data from consults consist of detailed consultants' notes and professional transcriptions of audio recordings made during consults. All participating clients consented to the use of records from their sessions in research. In total, we analyzed data from 24 consults with 23 clients (one client returned for a second appointment). Transcriptions were scrubbed of any possibly identifying information prior to analysis.

In parallel, during August 2020, we conducted five focus groups with seven volunteer consultants who participated in the remote delivery of consults. Three of the focus groups focused on consultants *general opinions and experiences* delivering remote consults to clients. One focused specifically on *changes* that consultants perceived between in-person and remote consults, and the other focused on *scheduling and administrative work* associated with ensuring remote consults could take place. Each type of focus group had a separate topic guide, with specific questions that probed the separate issues being discussed (all focus group guides are provided Appendix A). Depending on their experiences and role in the tech clinic, the volunteer consultants participated in between one and three focus groups each.

Each focus group had between two and four participants. We did our best to make participants feel comfortable sharing their experiences by ensuring equitable power dynamics within each focus group, including not placing managers in the same focus group as their direct reports. Each session lasted 90 minutes. With participants' permission, focus groups were audio-recorded, and recordings were professionally transcribed and anonymized.

Participants. Our client participants consisted of 23 women. Consults were conducted in English and Spanish based on client preferences. All clients were referred to CETA by their FJC advocate.

Our consultant participants included six women and one man, with levels of experience in the clinic ranging from six to 22 months. Four of the seven volunteered in both in-person and remote settings. Three consultants were responsible for scheduling client consults as part of their volunteer work in addition to consulting with clients. Four of the consultants are also authors of this paper.

Data analysis. We analyzed our notes and transcripts from consults and focus groups using a bottom-up thematic analysis approach [6]. We began with detailed readings of each piece of data, allowing initial codes to emerge. Three authors independently reviewed six transcripts. Through six rounds of iterative coding and reconciliation, we refined our codes into two codebooks: one focused on consultants' reflections, derived primarily from the focus groups and from reflexive sections of consultants' notes, and a second codebook focused on the consults themselves, derived primarily from the consult transcriptions and descriptive sections of consultants' notes. Examples of codes from the former codebook include *client satisfaction*, *consultant showing fallibility*, and *consultant as educator*; examples of codes from the latter codebook include *not enough time*, *pandemic impact*, and *unexpected interruption.* After the six rounds of reconciliation, the codebooks proved to be stable and subsequent coding was split evenly among three of the authors. We then performed multiple passes over the two codebooks to further refine and merge them into a unified set. Our final codebook (Appendix B) consisted of 65 codes clustered into nine high-level themes.

Safety, privacy and ethics. We were sensitive to the challenges of working with IPV survivors, a vulnerable population, as well as the challenges of studying a volunteer-staffed support service. Our study design placed great emphasis on ensuring participants' safety and privacy. Principally, we ensured that participation in this study would not result in greater risk for survivors than the risk associated with seeking help from the tech clinic in the first place. As described in other sections, we assessed client safety prior to an appointment; enforced anonymity for both clients and consultants; and encouraged clients to safety plan with an IPV professional before making changes to any devices or accounts.

When collecting data, we took care to not record any identifying information. In addition, we further anonymize quotes and stories from clients and consultants by paraphrasing and removing potentially unique phrases where needed. Any tools and apps mentioned by name are very common; the names of any esoteric tools or apps have been removed.

We also recognize that working with IPV survivors can be challenging, and that reflecting on the risks of the work amidst a global pandemic can stir emotion. Our research did not record or interrupt consultants' existing procedures for debriefing after consults, and did not interfere with the mental health services to which consultants are already provided access. In addition, we made clear during our focus groups that participants were free to step away at any point, or refuse to answer a question, for any reason. Finally, participants' responses in our focus groups were anonymized to protect volunteer consultants' responses from re-identification by their managers.

Limitations. It is important to note the specificity of our research context. The clinic in our study operated in an urban environment, and relied on survivors' ability to at least communicate over phone and email. Our study offers some common learnings for other technology-focused IPV support services, but should not be assumed to neatly generalize to survivors and support services in rural contexts, or to survivors who may be unable to communicate via digital technologies at all.

Similarly, it is important to note that our study has limitations with regard to intersectionality. Existing literature has advanced that support services should take an intersectional approach to better meet survivors' needs [47]; however, in the interest of maximizing client safety, we did not collect, store, or attempt to infer demographic attributes like age, race, or socioeconomic status. Gender indicators in the form of clients' preferred pronouns were used only to facilitate communication, and were received from the client's case worker during appointment scheduling (e.g. "She has a safe device"). We look forward to future work that can safely collect this information from clients, with the goal of analyzing the experience of remote IPV support services for victims with particular identities.

5 FINDINGS

Amidst the onset of citywide shutdowns due to COVID-19 in March 2020, CETA quickly adapted its volunteer-staffed computer security service from in-person to remote delivery. In doing so, it was able to support survivors grappling concurrently with the pandemic and with tech abuse. Many clients expressed gratitude for these ongoing services:

> *"Thank you. I really wish that this were a little more readily available for people because I feel like this is kind of a big deal, tech abuse. I'm really so appreciative that you guys do it."* (Client-20)

Our analysis found that mounting this remote computer security service required addressing a number of fundamental challenges. First, we found that the switch to remote services created new tensions around assessing and maintaining safety for clients and consultants (5.1). We additionally found the remote context imposed limitations on how device security investigations could be conducted, requiring consultants to adapt their procedures (5.2). Finally, we found remote service delivery created new burdens for consultants around the time commitment needed, as well as the mental and emotional requirements of the work (5.3). We describe each of these in turn.

5.1 Rethinking safety for clients & consultants

A principal concern throughout our findings was how to ensure safety for both clients and consultants. Clients experiencing tech abuse risk escalating harms if their abusers discover they sought help. For example, an abuser who finds a survivor has reached out to a support service might cut off their access to email to prevent them from further correspondence, or respond with physical intimidation or violence. IPV support services also grapple with how to ensure mitigation steps taken during an appointment do not themselves endanger the client. For example, discovering and uninstalling a location tracking app that an abuser has placed on a client's phone risks alerting the abuser, further endangering the client.

The circumstances of remote support delivery amidst a pandemic exacerbated these concerns. Whereas clients may have been able to visit FJCs or contact case workers secretly in pre-pandemic times, social distancing and stay-at-home orders mean that clients may be locked down with their abusers. Even clients who are able to find a private place from which to call a case worker face significant risks: Clients often have no choice but to call on the very devices they suspect may have been compromised. In parallel, consultants also face some degree of risk, in particular the potential exposure of their names, faces, or personal information to abusers who might be listening. In the worst case, one consultant said, an abuser might retaliate against people supporting their victim, and use information about a consultant gleaned through leakage on a call to find them and enact violence against them.

To mitigate the risk of an abuser preventing a client from seeking help, listening in on an appointment, or retaliating against either client or consultant, the remote support service in our study utilized a range of safety and anonymity measures briefly described in Section 3. In this section, we detail these measures in two groups: (1) safety self-assessments done before an appointment, and (2) protocols for maintaining safety during and after a consult. For each, we describe what our study revealed about how the measure was designed, and how consultants felt it played out in practice.

Assessing client safety prior to a consult. A key piece of ensuring safety in the remote consults was an assessment conducted during the client intake process. In addition to asking the referring IPV case worker to describe the client's overall problem, the intake form asked if the client had (1) a *safe location* from which to call in, and (2) a *safe device*, meaning one to which the abuser had never had physical access. Case workers who answered no to either or both of these questions were asked to work with the client to procure a safe device and a safe location from which they could take a call. To account for last-minute changes to clients' safety situations on the day of the call, consultants additionally confirmed at the start of each consult whether the client was calling from a safe location on a safe device.

Our data show that in practice, these assessments were used less as a filter for consults that might be too dangerous to proceed, and more to encourage clients to consider the risks of engaging with support services and occasionally take extra steps to be as safe, if they could. In some cases, clients halted a consult to call in on a different device, e.g., a work laptop. In others, clients could not be certain whether their device was considered safe, but gave consent to proceed regardless and, in line with a client-centered approach, consultants acceded.

Reflecting on these assessments in our focus groups, several consultants expressed that the process of doing the checks laid bare for them the uncertainties around clients' safety, and made apparent the potential risks to their own privacy that are inherent to IPV support work. As one consultant described, the safety checks raised new issues around control:

> *"In the in-person setting, we very intentionally built ourselves into the FJC infrastructure, so we had the advantage of the safety apparatus set up there. When we're remotely contacting clients, all we can really do is trust they're out of danger, and say, 'Okay, great. You've told us that you're in a safe location, that you have a safe device.' We don't have that very real material control over what the setting is."* (Consultant-04)

For this consultant, the security afforded by physically working within the FJC infrastructure appears to have created sufficient assurances of safety, in that they lent a sense of control over the risks of IPV support work. Those physical assurances were absent in the remote context, heightening this consultant's concerns around safety. Consultants in our focus groups generally agreed that working at the FJCs had lent a greater sense of safety—with the important caveat that the FJC environment, which typically requires visitors to register at a front desk and screens entrants through a metal detector manned by uniformed police, may in some cases provide cause for alarm rather than assurances of safety. Survivors who are members of communities marginalized by the legal system, e.g. Black people [40, 82], may experience these security measures differently, consultants noted. For anyone who may have been uncomfortable in the in-person setting, consultants pointed out that remote delivery may in fact have been beneficial: providing or accessing services in their homes or other non-FJC contexts may have actually felt more controlled.

Another consultant, however, said the fact that safety assessments occurred pre-consult in the remote context actually mitigated risks relative to in-person consults. Doing safety checks provided more information on potential compromises than was available prior to an in-person consult, and this in itself provided a greater sense of control:

> *"[In the in-person context] there were many times that people came in with compromised devices, living in very scary situations, telling us very real threats happening to them and their families. And there we were with that device that the abuser appeared to have access to. I think we do much more now to ask these questions, where before we assumed someone was coming in with an unsafe device."* (Consultant-03)

As this consultant highlights, the nature of tech-mediated IPV is such that the risk of encountering a 'hot' device—one on which the abuser is actively listening or recording a client's activities, through spyware or other means—is such that support workers must assume a device has been compromised and proceed accordingly. The safety checks, therefore, served to provide information on potential risks above this baseline. Throughout our focus groups, consultants agreed that having more information on clients' situations prior to an appointment was preferable, even if that information indicated above-baseline risk that an abuser might listen in. To another consultant, the utility of the safety checks was also to create space for clients to make informed decisions about the risks associated with seeking out support services:

> *"My sense is that from the perspective of the client . . . it seems like a wash. Some clients are going to have more risk coming in-person. Some clients are going to have more risk on the phone. I'm hopeful that we can have it so that clients can make informed decisions about their risks of even getting in touch with us."* (Consultant-02)

To this consultant, the safety checks were a way to make clear to the client what the risks of seeking help might be in any service context. Neither in-person nor remote contexts entailed greater risks: the risks were simply different, and ultimately the decision of what risks to assume was up to the client. We unravel these issues further in Section 6.

Maintaining safety during a consult. Consultants also took steps on each call to ensure consults remained safe for all participants. First and foremost, consultants took care to **preserve anonymity**. Consultants ensured real names were not used on the conference call platform, and verbally referred to each other using an alias—typically *"my colleague"*. Clients were reminded to refrain from sharing their own names or identifying information. Sessions were conducted via audio only to prevent leakage of faces, homes or physical locations.

Our data suggest consultants generally perceived anonymity to be a valuable safety measure that provided them with a sense of control over the consult. But this measure also, at times, lent a stilted air to on-call interactions. Clients sometimes accidentally divulged names or identifying details like email addresses, to which consultants would jump in with a gentle reminder, e.g. "*we don't use names here*". These policies also created, at times, moments of levity: consultants often verbally handed off to each other using an alias, e.g. "*My colleague, is there anything I've missed?*", sometimes eliciting a chuckle from the client. We unpack further tensions introduced by these measures in Section 6.

Another key element of ensuring safety was the ability to conduct proper **safety planning**. As described in prior work [44], safety planning involves calling the referring IPV professional in the event that a consult surfaces active device or account compromise. The referring professional then joins the consult to advise on the potential implications of any mitigation steps. Involvement from IPV professionals is critical because, as one consultant said, CETA trainings do not cover crisis situations:

> *"We're not domestic violence hotline counselors. We haven't trained for the scenario of somebody calling us who could suddenly be in acute danger, or face an significant safety threat right then."* (Consultant-01)

Our data show consultants were concerned about their ability to properly safety plan in the remote context, since access to trained crisis professionals was diminished. While support workers were not always physically present in the in-person context, in the remote setting, when all parties were distributed and, in many cases, working from home, consultants felt even less of a sense that support workers were reachable. As one consultant described:

> *"We can't go down the hall and ask for help [from a support worker]. That has to be handled asynchronously. And my suspicion is that it's not being handled nearly as well, since it's harder to get in touch."* (Consultant-02)

These difficulties constitute a particularly noteworthy challenge, as safety planning is often critical for clients' and consultants' peace of mind. We discuss these tensions further in Section 6.

5.2 Assessing device security remotely

As described in Section 3, CETA's in-person consult protocols adopted the *Understand-Investigate-Advise* (UIA) framework reported in prior research [36, 44]. Our analysis shows the remote context posed significant challenges to the *Investigate* phase: without the ability to see and touch a potentially compromised device, or connect it to a spyware scanning tool, consultants were forced to adapt many of the instruments they had previously used. We begin this section by outlining what our analysis revealed about the limitations to the *Investigate* phase created by the remote context. We then discuss what we learned about consultants' adaptations to these challenges.

Limitations on device and account investigations. Throughout our data, we encountered a fundamental challenge of remote security assessments: a reduced ability to interact with the devices or accounts in question. As discussed previously, **lack of visibility** was implemented as a safety measure—clients and consultants were most able to maintain anonymity if the consult was limited to a call with no video on either end. This differed significantly from in-person consults, where both parties would be able to look at a screen together, and a consultant could, with a client's permission, touch a device. This change had the clearest impact on the more programmatic elements of investigation, for example the spyware scanning tool reported in Havron et al. [44] that required consultants to connect to the device over USB.

An inability to use programmatic spyware investigation tools does not necessarily render consults ineffective. Previous reports suggest spyware is found in a very small number of cases [44], and that much of a UIA consult's value can be derived from other investigation techniques: In-depth interviews and manual account privacy checkups are often sufficient to help clients "connect the dots" on how their abuser might be causing harms, and most clients leave consults with proactive advice on security best practices [36]. However, despite consultants' efforts to inform clients that spyware is a rare and unlikely risk, throughout our data we found that clients came to a consult specifically seeking information on whether spyware had been or was currently on their phones:

> *"So you guys actually wouldn't be able to tell me . . . would you be able to tell me if there was some spyware, or are you just helping me avoid it?"* (Client-15)

To approximate checks for spyware and other sources of compromise, consultants guided the client through their devices or accounts by having them navigate their interfaces and describe out loud what they were seeing, for example reading out loud the list of apps installed on their devices (we provide an example below). Clients in our data were generally able to execute these checks; however, consultants said they often created new difficulties:

> *"The biggest problem is when we do these manual checks. We can't see the list of apps on their phone, so they have to read out all the apps to us. It can be overwhelming, and it also feels more uncertain."* (Consultant-07)

In addition to overwhelming clients or creating uncertainties for consultants, these checks were also often inefficient. For one, **connection problems** on either the consultants' or the client's end sometimes made it difficult for them to hear each other, or dropped calls entirely. In some cases, clients had difficulty joining the conference line in the first place, delaying the consult by up to 20 minutes as consultants reached out asynchronously to the case worker to figure out how to connect them. Even on consults where both parties managed to connect, remote navigation posed challenges due to clients' and consultants' **differing levels of familiarity with specific devices and terminology**. In the example below, a client with a Windows laptop and consultant who is a Mac user attempt to locate the Settings menu on the client's laptop:

> Consultant: *"There should be a button, usually in the lower left. Unfortunately I can't see your screen so I can't tell you exactly where to click. But there's usually a big button in the lower left-hand corner with a little Windows icon on it. It's like a little square."*
> Client: *"Where I see a Google Chrome, Microsoft Edge, those? Zoom, Office Word, Fire Explorer. . . that?"*
> Consultant: *"I think so. Do you see a Settings button?"*
> Client: *"No. I don't know. I'm not too good with this, the technology."*
> Consultant: *"Okay, hmm. Give me a second, I'm trying to look this up so I can help you a little bit more."*

Here we see both parties struggling to align on a shared language for describing the interface of the client's laptop. Compounding the confusion is the consultant's unfamiliarity with the client's system: Where they may have been able to visually navigate an unfamiliar interface in-person through common visual cues, in this context they could rely only on a client's description. Consultants in our focus groups agreed that their own unfamiliarity with apps and platforms they did not use personally often made remote navigation particularly difficult.

Our analysis also found that consults were sometimes delayed by **external interruptions**. In five of our 24 consults, a session was paused for an interruption by a client's child or friend, or by the client receiving another call. We attribute these delays to the fact that clients and consultants alike were taking calls amidst New York City's COVID-19 lockdowns: it was a challenge for anyone to find a private place from which to take an hourlong call.

While connection, interpretation, and interruption problems like these are inherent to any phone-based support service, our analysis found that remote navigation procedures also created challenges related to the management of clients' **emotional stress**. Consultants were keenly aware that for some clients, attending a consult was a stressful event, requiring them to remember traumatic experiences. They were also attuned to the added burden of navigating through unfamiliar or opaque interfaces—on devices through which an abuser may be harassing them, and while listening, processing, and attempting to follow consultants' instructions. Consider the following paraphrased example, in which a consultant attempts to guide a client through a Google privacy checkup:

> Consultant: *"Could you open Chrome or Safari or whatever you use, and type in myaccount.google.com?"*
> Client: *"Okay."*
> Consultant: *"Then sign in with the email you want to focus on now. Just let me know when you're ready."*
> Client: *"Yeah. It's not pulling it up. Sorry."*
> Consultant: *"That's okay. Just so you know, it's myaccount, one word, and then dot-google-dot-com."*
> Client: *"I know. It's asking for the password and I'm trying to. . . my hands are super shaky."*
> Consultant: *"No problem at all, take your time. It sounds like you've been through a lot."*

Here, the consult is delayed to account for the consultant's perception that the client is expressing stress. Moments like these occurred frequently in our data, and in response, consultants consistently made space for clients to take their time locating account options or remembering passwords. Clients seemed particularly sensitive to the idea that they were somehow failing if an appointment ran out of time:

> *"I had a 9 a.m., a 10 a.m., an 11 a.m., a 1 p.m., a 2 p.m. . . . I just have to get through this because I don't have any other time. I know how hard it was to get this appointment and I don't want to blow it."* (Client-5)

In response to concerns like these, consultants took steps to reassure clients, e.g. by reminding them it would be no problem to schedule a second appointment. Throughout, consultants remained highly attuned to clients' emotional expressions, and calibrated their own words and tone of voice accordingly. We further unpack consultants' attention to clients' emotional needs as a form of emotional labor in Section 6.

These inefficiencies culminated in what had, by the time of our focus groups, become conventional wisdom among consultants: In comparison to in-person consults, when one could expect to guide a client through multiple problems with multiple devices, remote consults were narrowed to investigations of at most one device or account per call:

> *"In-person we could handle anywhere from one to maybe seven devices. You could go through a lot of devices with two or three people in that room. Now, we really are doing much more of a one-off on one device. I really haven't had the luxury of handling more than one device in a call."* (Consultant-03)

This represented a reduction in efficiency from in-person to remote consults. To account for this, consultants altered their practices regarding what could be investigated in an appointment. We now describe some of those adaptations.

Adaptations for remote security assessment. Consultants adapted to the demands of conducting device and account security assessments remotely by (1) encouraging a client-consultant dynamic weighted more towards collaboration and facilitation than expert guidance, and (2) relying on follow-up emails after a consult to convey important next steps.

As described above, the remote and audio-only context forced consultants to find ways to compensate for a lack of ability to conduct spyware scans and privacy checkups with the device in hand. Instead, consultants guided clients through navigating their devices remotely by having clients read out loud what they saw on their devices. Reflecting on these processes, consultants in our focus groups agreed that remote navigation resulted in a shift in the consult dynamic towards **client-consultant collaboration**. In-person consults had been collaborative, too, but the nature of these manual checks meant remote consults required more active involvement from the client. Whereas in-person consults may have consisted largely of consultants "*taking the reins*" and performing device checks on a client's behalf, the remote setting created opportunities to cultivate a feeling of empowerment for clients:

> *"Because we're not doing things for the client, for clients that do have some ability to navigate settings and so on, we actually wind up teaching more. Showing them, empowering them more to be able to have the knowledge to handle some of these things themselves, and to have the confidence as well."* (Consultant-01)

The theme of consultants providing opportunities for clients to feel empowered to handle their own device security recurred across our data. Several consultants mentioned this was particularly important in the gendered context of IPV: The coercive control characteristic of tech abuse [23, 68] means abusers often seek to disempower their victims by creating barriers to technological self-determination. One consultant pointed out that since the clinic's clients are overwhelmingly cisgendered women, clients' feelings of disempowerment where technology is concerned are often compounded by the stereotype that women are less technically competent than men. (We unpack further the implications of this observation in Section 6). In the face of these societally reinforced inequities, consultants felt that providing clients hands-on opportunities to learn about their own devices was valuable.

Consultants also encouraged clients to set the agenda of a consult, in accordance with a client-centered approach. In practice, this often meant consultants would ask clients which device or concern they wanted to start with. As one consultant said, this was partially an efficiency measure to account for the fact that consults requiring remote navigation simply took longer; however, it also created opportunities to give clients a greater sense of control:

> *"I know I might not be able to get to everything and I always want to check with the client to make sure that we're helping them, and they feel empowered, and we're attending to their greatest needs."* (Consultant-03)

While attention to empowering clients had been a focus within in-person protocols as well, consultants agreed it took new urgency under the remote paradigm. We unpack the prospect of empowering clients in Section 6.

Throughout our data, we also found that consultants expressed an increasing reliance on **referring clients to follow-up emails**. In this practice, consultants would take time post-consult to compile resources on topics not covered in the session, but identified to be extremely relevant to a client's case: e.g., links to reputable antivirus software, or instructions on how to check the devices logged into an iCloud account. These resources were sent via email to the client's case worker, who would then forward them to the client. The practice of compiling and sending follow-ups had been used in in-person contexts, but consultants expressed they had been used far more sparingly.

Providing more information via post-consult emails also had the effect of encouraging consultants to systematize the production of written advice. Instructions on turning on two-factor authentication, for example, were often issued across clients. To standardize these communications, consultants began creating **written how-to guides** for clients to follow on their own. Developed to convey information in visual- and text-based formats, these guides are written for use by anyone to check security and privacy settings across platforms and apps. Guides include, for example, checklists for how to disconnect from an abuser on shared technology platforms such as Spotify or Netflix (platforms often overlooked as sources of entanglements). In some cases, these guides were adaptations of internal materials previously written by consultants for use solely by other consultants, so making them appropriate for clients often required rewriting them to align with clients' tech literacy. We discuss the prospect of clients using these guides in Section 6.

5.3 Handling new burdens

Finally, our analysis found the transition to remote services created new burdens for consultants, many of which were attributable to the distributed nature of the work. Consultants voiced these increased burdens in two broad themes: (1) the sheer amount of *extra work* required to deliver consults remotely, compared to in-person; and (2) the *emotional tax* to consultants of doing the work, most often frustration at the limits of the remote setting.

Remote service delivery requires substantial extra work. Prior to the switch to remote appointments, consultants had worked on the basis of volunteering for set half- or full-days on-site at an FJC, seeing a maximum of four clients per day. To minimize secondary traumas accumulated from doing too many sessions, volunteer consultants worked at most one or two days per month. Separating from the in-person paradigm enabled CETA to explore the possibility of offering appointments via a more ad hoc model, with consultants volunteering for appointments scattered throughout the week. This procedural switch offered tantalizing benefits for the possibility of broadening access to services, making consults available to clients in a diverse range of circumstances.

However, consultants expressed that this change had the effect of multiplying the work and time required to complete their caseloads. First, recall from Section 3 that consult teams often met before and after the 60-minute appointment, to first prepare and assign roles and then to debrief and assign follow-up work. These pre- and post-meetings ranged from 15–30 minutes, depending on the consult team and the complexity of the case. As one consultant articulated, these meetings played a significant role in helping consultants feel prepared for consults and relieving their stress after:

> *"I feel a lot better if I prepare properly for the consult, so spending a full half hour getting organized beforehand helps quite a bit. And then chatting afterwards does help me as well, it is a good outlet."* (Consultant-02)

Moreover, remote appointments tended to require the production of follow-up emails and written guides more often than in-person consults. Consultants in our study estimated this follow-up work added two or three hours to the work put into each consult, with high variance due to the fact that some topics required more or less research, or rounds of edits with team members. This additional work presented particular challenges, consultants said, because in the remote paradigm they were often required to task-switch in and out of consults while balancing other work and family demands. Whereas in-person clinic work had been structured as a full day on-site at the FJCs, spreading appointments and follow-up work throughout a consultant's week created significant additional mental overhead. Reflecting in the focus groups, one consultant said: *"The cognitive burden of having one appointment a day is almost similar to having four appointments a day, right?"* (Consultant-03). Consultants acknowledged these tensions may have been exacerbated by the circumstances of the pandemic—for example, some consultants in our focus groups had to balance their work duties against caring for children who were also under stay-at-home orders. Still, consultants across all circumstances agreed the basic premise of scattering appointments throughout a week created significant stress.

Remote service delivery is emotionally taxing in new ways. Our data additionally show that delivering these services over remote connections created new emotional strains on consultants. At issue was the emotional labor of providing reassurance to clients amidst circumstances challenging for both parties. As one consultant described, providing emotional expressions like validation and connection often constituted an important part of a consult:

> *"I think clients now—they're in horrible situations, they're isolated. So just having interaction with a human who's dedicated to helping them, I find people are very appreciative."* (Consultant-03)

Providing this type of reassurance, however, was uniquely challenging in the remote setting. Consultants lacked many of the empathetic cues they would have used in-person to convey warmth. As one consultant articulated:

> *"If a client is becoming distressed during the in-person appointment, there are things we can do to show empathy, and show we care. And give them that breathing space, and respond. We can do things like offer tissues, offer water, and be a more reassuring presence. Over the phone, remotely, that's a lot harder."* (Consultant-01)

Consultants used a range of strategies to approximate the reassurance they might have provided in-person. For example, some consultants halted consults in moments where the client seemed to be overwhelmed, encouraging them to *"stop and take a breath"*. The emotional work of providing reassurance over the phone, to clients in uniquely *"horrible situations"*, was compounded by consultants' own feelings of frustration over the inherent uncertainties of the work. For some, having to conduct device security assessments over the phone reduced their own sense of competence. While they were aware of the prior work showing programmatic tools rarely surface vulnerabilities [44], they felt being unable to use these tools made it harder to create a dynamic of trust within the appointment: *"I feel way less capable. It's harder to convey competence to the client and convince them to trust me"* (Consultant-04).

Other consultants felt their inability to use programmatic tools may actually have benefited the collaborative dynamic and client empowerment goals described in Section 5.2. As one consultant articulated, the remote setting created a sense of parity between client and consultant—and importantly, in their estimation, clients did not seem perturbed:

> *"It can be healthy that the remote setting is perhaps more egalitarian. We all ought to be comfortable saying that we don't know something, or taking time to look for something. Clients have been quite understanding when we say, 'Actually, I need to take a moment to discuss this with my colleague or sort this out.' "* (Consultant-01)

The theme of managing clients' expectations recurred throughout our data as an additional source of frustration for consultants. While an examination of clients' own perspectives on their satisfaction is beyond the scope of this work, our data show consultants themselves grappled with whether they were truly able to help. As one consultant said:

> *"At first, I thought that if we really found where the problem is, then that would make a session successful. But it's hard to find out the exact problem, so instead we examine the devices and help them set up extra security. It's hard for me to really classify whether it's successful or not."* (Consultant-07)

Consultants agreed that handling these uncertainties and managing clients' expectations in the face of them was difficult, but inherent to the work. As one consultant described, accepting the limitations of the service was often frustrating for all parties—particularly in the context of a free service specifically dedicated to IPV-sensitive tech support: *"When we're not able to help, I think that's hard for everyone"* (Consultant-01).

Finally, managing the emotional tenor of these consults was taxing for consultants not just due to the difficulties of empathizing with clients remotely, but also due to stress the pandemic placed on consultants themselves. CETA trainings included sections on managing compassion fatigue and secondary trauma, but many consultants' coping mechanisms—e.g., exercise, counseling, social outlets—were made impossible by NYC's shutdowns. Further, as one consultant said, there was a marked similarity between lockdown and the very abuses consultants worked to mitigate:

> *"Pandemic lockdown can be very reminiscent of abuse, in the sense of isolation, fear, and being cut off from people you care about. We're trying to provide this service in a situation where we may all be experiencing some of the cognitive and psychological challenges of something very much like an abuse situation, with fewer resources for maintaining a healthy, productive service."* (Consultant-01)

As this consultant points out, the particular circumstances of COVID-19 may have created conditions ripe for inducing compassion fatigue and secondary trauma among consultants. In Section 6, we unpack further the challenges consultants faced managing their own reactions in the course of their work.

6 DISCUSSION

In this section, we begin by highlighting three key tradeoffs with which the consultants in our study grappled, each of which is broadly relevant to the provision of any expert service over a remote connection: (1) the balance between safety and efficiency; (2) the balance between emotional and technical work; and (3) the balance between empowering or enabling clients and creating new burdens. We provide recommendations for remote support providers within each, and close with key areas for future work in computer security services for IPV survivors specifically.

Balancing safety against consult efficacy. Sections 5.1 and 5.2 discuss how the tech clinic in our study strove to ensure safety for clients and consultants in the face of the fundamental dilemma of remote security assessment: how to use potentially insecure devices to try to secure them. This was done primarily through measures to assess clients' safety before each session, and to preserve anonymity throughout each consult. To our consultant participants, these measures aimed to mitigate risks including: (1) that the abuser learns the client has sought help, and retaliates against the client; (2) that the abuser listens to the consult and finds ways to circumvent the security recommendations given; and (3) that the abuser learns a consultant's identity and retaliates against them.

Consultants in our study acknowledged that current procedures have no way to *guarantee* that an abuser is not actively surveilling a client — clients are, after all, often seeking an appointment specifically to help investigate their suspicions of surveillance. The safety measures were nevertheless perceived to have positive impact on mitigation of all three of these risks: Consultants felt they encouraged clients to take safety precautions and helped them be more informed and proactive in handling their situation. This was a positive outcome for a client-centered approach. In particular, consultants viewed that preserving anonymity provided them with notable security benefits where risk (3) is concerned. This perception is important for consultant well-being, regardless of the actual risk of retaliation against consultants: Indeed, while we are unaware of studies measuring the prevalence of retaliatory harassment or violence targeted specifically at support professionals, prior work has documented that they can suffer collateral damage when abusers track survivors to the physical location where in-person support is being provided [42, 56].

The benefits of safety measures must be weighed against our findings that they created barriers to clients accessing the service (e.g., having to procure a new phone or take a call from work) and hampered consultation efficiency. Some measures, like not using names during a consult, created minor inefficiencies. Others, like the audio-only remote navigation procedures, created frustrations so time-consuming that they severely limited the number of devices that could be checked in an hourlong appointment. Protecting clients and consultants should, of course, be a first-order concern, but future work is needed to understand how to appropriately balance safety and consultation efficacy.

We suggest one route towards improvements: consultative services that support a plurality of remote delivery modalities and associated safety measures. In our Findings, we saw that broadly issued guidance led to a one-size-fits-all policy that made balancing safety and efficacy difficult. Enabling tailored solutions could, for example, provide the option of relaxing constraints by enabling face-to-face video calls for consultants less concerned about re-identification and more for the rapport-building afforded. Tailoring by default would also provide a way to account for the variance in clients' risk profiles, and even the inherent variability in how case workers might assess client risk.

Balancing consultants' emotional and technical labor. Throughout our findings, consultants described how remote service delivery created novel emotional requirements: new skills to use with clients (e.g., actively checking in with them throughout a consult, or encouraging them through remote device navigation) and new skills they must use to manage their own reactions to the work (e.g., finding time to decompress after appointments). These are forms of *emotional labor*, described in the literature as a set of work demands regarding (1) targeted expression of emotion on-the-job, and (2) self-regulation of a worker's own emotions [4, 10, 54]. Prior work has shown emotional labor is un- or under-recognized in many client-oriented professions disproportionately occupied by women, for example nursing and retail, and correspondingly un- or under-compensated [69].

While the pandemic context certainly exacerbated emotional burdens, our findings indicate that the emotional labor inherent in support services is heightened in remote contexts. This has direct implications for scaling consultation services: excessive emotional labor has been linked to burnout [10]. Mitigation strategies such as measuring and treating compassion fatigue have been proposed in social work and psychotherapy [8, 32], but the particulars of the emotional labor in remote consultative work delivering computer security assistance present unexplored territory. Technologists who develop expertise in computer security and privacy do not concurrently develop expertise in emotional labor by default: there is no equivalent of the clinical skills training provided in medical or social work programs. Context-switching between the provision of technical security advice and emotional reassurance may create new difficulties, requiring new sets of evidence-based best practice. Further work is needed to illuminate the precise contours of the emotional labor needed in computer security consultation settings, and develop new best practices. In addition, further work is needed to develop organizational structures for recognizing emotional labor, particularly as the future of work shifts towards distributed forms of remote collaboration. Such work might build on the literature advancing frameworks for the evaluation of emotional labor in in-person work [69], and construct organizations that incorporate its acknowledgement into compensation structures and pathways for advancement.

Balancing client enablement against new burdens. Our work also highlights a tension of remote service provision that is of particular interest to technologists working to support vulnerable people: the prospect of *empowering* clients to conduct privacy checkups themselves. As discussed in Section 5.2, consultants feel the remote setting shifts the in-consult dynamic towards one of *collaboration*, in which clients, not consultants, conduct most of the investigation and set the terms of the conversation. An important goal of a consult, several consultants said, is to leave the client capable of protecting their own digital security and privacy—an outcome particularly important for women facing abusers who are men, since these abusers are known to take advantage of the stereotype that men have more technical capabilities than women [23, 68]. While consultants in our study describe this as "empowerment", we believe it is better described as *enablement*, or the facilitation of "*opportunities for people to develop their own capacity*" [22]. As Erete et al. [28] write, technology interventions alone cannot empower people to solve social problems without addressing underlying inequities across communities. People become marginalized at the hands of oppressors who hold power where they do not, and to describe projects as empowering when they do not truly shift power can obscure these effects.

Reconceptualizing this intervention as an instance of enablement creates a lens for its potentially negative effects: enabling marginalized people through the provision of technological systems or knowledge can have the effect of creating new, unwanted burdens for them to handle [22, 76]. In our context, we find that consultants' goals of enablement may at times be at odds with the possibility that consultations burdened survivors. Bolstered by the knowledge of how to counter vulnerabilities surfaced during a consult, clients may indeed be enabled to wrest some power back from their abusers, but their actions may also incite further harms requiring further work to mitigate. Moreover, maintaining personal digital security is laborious, and clients may face a steep learning curve—and for women facing abuse by men, these burdens can be compounded by the same gendered dynamics that created conditions for their abuse in the first place. From the perspective of technologists mounting these interventions, we ask: How do we reconcile our role enabling the client with the potential of these procedures to create additional burdens, or even new forms of abuse requiring more intervention?

As a first step to unpacking these complications, we suggest further work examining the more long-term effects of these consult procedures, including assessments of how the consult and the associated resources (e.g., written guides) impact clients' situations beyond the consult itself. For example, knowledge of when and whether clients used these guides on their own might help us disentangle whether this technology intervention created additional unwanted burdens for survivors, or helped them develop the capacity to achieve their goals.

The future of remote assistance for IPV survivors. The clinic at the center of our study developed its remote consultation protocols quickly, as a form of crisis response. Transitioning in-person services to remote delivery over general-purpose tools for computer-mediated communication—while handling social upheaval during COVID-19 in spring 2020 in NYC—made these important services immediately available to survivors, but these procedures were not necessarily intended to persist or scale beyond this setting.

Our findings chronicling the challenges faced in mounting this service contribute knowledge that can inform the development of safe and effective computer-mediated support services for vulnerable people—lessons that become more relevant as cities around the U.S. consider reopening. At time of writing in September 2020, FJCs in NYC were still closed indefinitely, but a history of rapid changes in the city's COVID-19 response indicate a reversal could happen at any point. In the event that FJCs were to re-open, inviting services to resume in-person, the clinic in our study would face an important question: Would services persist in the remote model, revert to the in-person model, or blend into a hybrid model to try to preserve the best of both modalities?

Our findings suggest that the remote service model does provide meaningful benefits. Many clients in our data may not have been able to attend an in-person appointment, due not only to the social distancing and lockdown measures required by COVID-19 but also to childcare or caretaker duties, work schedules, and other obligations that make traveling to an FJC during a business day impossible. Offering a remote option would do a lot to help these clients, and perhaps many other survivors currently less able or inclined to seek in-person services at FJCs guarded by uniformed police: survivors in rural environments, LGBTQ people, and members of Black, Muslim and other communities who have been notably subject to police brutality [40, 82]. Making services available to these communities via remote delivery could increase their impact.

In addition, we imagine hybrid services would be particularly effective at broadening access to support when they can be tailored to the particulars of clients' and consultants' needs. Offering a plurality of communication modalities and safety mechanisms might in itself help; we also see compelling future work exploring triage mechanisms that might route clients towards one type of specialized support versus another. Adaptive and hybridized support services are a key starting point for an intersectional approach to remotely delivered victim services: one that can take into account survivors' particular linguistic, cultural, age and ability cohorts. In line with recent literature discussing how intersectional approaches are critical to meaningfully addressing victims' needs [47], we look forward to future work developing tools and approaches to working with each client's particular axes of oppression.

7 CONCLUSION

We report a qualitative study of how technologists with computer security expertise provided remote assistance to IPV survivors amidst citywide shutdowns due to COVID-19 in the spring of 2020 in New York City. Our findings reveal the delivery of these services raised tensions around three fundamental challenges: (1) ensuring safety for both clients and consultants over a computer-mediated connection; (2) assessing device security over audio-only communications; and (3) navigating the additional labors created by distributed work. We discuss how these tensions speak to tradeoffs that must be made in the provision of any remote support service, and provide specific recommendations for technologists interested in mounting similar computer-mediated support services for vulnerable people.

ACKNOWLEDGMENTS

This research was funded in part by NSF Award #1916096, as well as gifts from Facebook and Google. We sincerely thank all of our participants for lending their time and expertise, and additionally thank our reviewers for comments that greatly improved our paper. Lastly, we thank Heidi He and Anam Tahir for their assistance with our study.

REFERENCES

[1] Yusuf Akamoglu, Hedda Meadan, Jamie N Pearson, and Katrina Cummings. 2018. Getting connected: Speech and language pathologists' perceptions of building rapport via telepractice. *Journal of Developmental and Physical Disabilities* 30, 4 (2018), 569–585.

[2] I Elaine Allen and Jeff Seaman. 2013. *Changing course: Ten years of tracking online education in the United States.* ERIC.

[3] Apple. 2020. Official Apple Support. https://support.apple.com.

[4] Blake E Ashforth and Ronald H Humphrey. 1993. Emotional labor in service roles: The influence of identity. *Academy of management review* 18, 1 (1993), 88–115.

[5] Brittany Bice-Urbach, Tom Kratochwill, and Aaron J Fischer. 2018. Teleconsultation: Application to provision of consultation services for school consultants. *Journal of Educational and Psychological Consultation* 28, 3 (2018), 255–278.

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

[7] Gretchen A Brenes, Cobi W Ingram, and Suzanne C Danhauer. 2011. Benefits and challenges of conducting psychotherapy by telephone. *Professional Psychology: Research and Practice* 42, 6 (2011), 543.

[8] Brian E Bride, Melissa Radey, and Charles R Figley. 2007. Measuring compassion fatigue. *Clinical social work journal* 35, 3 (2007), 155–163.

[9] Laura Brignone and Jeffrey L Edleson. 2019. The Dating and Domestic Violence App Rubric: Synthesizing Clinical Best Practices and Digital Health App Standards for Relationship Violence Prevention Smartphone Apps. *International Journal of Human–Computer Interaction* 35, 19 (2019), 1859–1869.

[10] Céleste M Brotheridge and Alicia A Grandey. 2002. Emotional labor and burnout: Comparing two perspectives of "people work". *Journal of vocational behavior* 60, 1 (2002), 17–39.

[11] Andrew M Campbell. 2020. An increasing risk of family violence during the Covid-19 pandemic: Strengthening community collaborations to save lives. *Forensic Science International: Reports* (2020), 100089.

[12] Rebecca Campbell. 2013. *Emotionally involved: The impact of researching rape.* Routledge.

[13] Joht Singh Chandan, Julie Taylor, Caroline Bradbury-Jones, Krishnarajah Nirantharakumar, Eddie Kane, and Siddhartha Bandyopadhyay. 2020. COVID-19: a public health approach to manage domestic violence is needed. *The Lancet Public Health* 5, 6 (2020), e309.

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

[15] Despoina Chatzakou, Nicolas Kourtellis, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Athena Vakali. 2017. Measuring# gamergate: A tale of hate, sexism, and bullying. In *Proceedings of the 26th international conference on world wide web companion.* 1285–1290.

[16] Ok-Kyu Choi and Erin Cho. 2019. The mechanism of trust affecting collaboration in virtual teams and the moderating roles of the culture of autonomy and task complexity. *Computers in Human Behavior* 91 (2019), 305–315.

[17] Jan Coles, Jill Astbury, Elizabeth Dartnall, and Shazneen Limjerwala. 2014. A qualitative exploration of researcher trauma and researchers' responses to investigating sexual violence. *Violence against women* 20, 1 (2014), 95–117.

[18] Sasha Costanza-Chock. 2018. Design Justice: towards an intersectional feminist framework for design theory and practice. *Proceedings of the Design Research Society* (2018).

[19] Andy Crabtree, Jacki O'Neill, Peter Tolmie, Stefania Castellani, Tommaso Colombino, and Antonietta Grasso. 2006. The practical indispensability of articulation work to immediate and remote help-giving. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work.* 219–228.

[20] Ronald J. Deibert. [n.d.]. The Citizen Lab. https://citizenlab.ca/.

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

[22] Lynn Dombrowski, Ellie Harmon, and Sarah Fox. 2016. Social justice-oriented interaction design: Outlining key design strategies and commitments. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems.* 656–671.

[23] Molly Dragiewicz, Delanie Woodlock, Bridget Harris, and Claire Reid. 2019. Technology-facilitated coercive control. *The Routledge international handbook of violence studies* (2019), 244–253.

[24] Carolyn Ellis and Art Bochner. 2000. Autoethnography, personal narrative, reflexivity: Researcher as subject. (2000).

[25] Chuka Emezue. 2020. Digital or digitally delivered responses to domestic and intimate partner violence during CoViD-19. *JMIR public health and surveillance* 6, 3 (2020), e19831.

[26] Technology enabled Coercive Control Working Group. [n.d.]. TECHNOLOGY-ENABLED COERCIVE CONTROL WORKING GROUP, SEATTLE, WA, USA. https://teccworkinggroup.org/.

[27] NYC ENDGBV. 2019. NYC Mayor's Office to Combat Domestic and Gender-Based Violence. https://www1.nyc.gov/site/ocdv/about/about-endgbv.page.

[28] Sheena Erete and Jennifer O Burrell. 2017. Empowered participation: How citizens use technology in local governance. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* 2307–2319.

[29] Sheena Erete, Aarti Israni, and Tawanna Dillahunt. 2018. An intersectional approach to designing in the margins. *Interactions* 25, 3 (2018), 66–69.

[30] Operation: Safe Escape. 2020. About Us - Operation: Safe Escape. https://safeescape.org/about/.

[31] Rose Eveleth. 2015. How to deter doxxing: newsroom strategies to prevent the harassment that can follow public posting of personal information. *Nieman Reports* 3 (2015), 46.

[32] Charles R Figley. 2002. *Treating compassion fatigue.* Routledge.

[33] NYC FJCs. 2019. NYC Family Justice Centers. https://www1.nyc.gov/site/ocdv/programs/family-justice-centers.page.

[34] UC Berkeley Center for Longterm Cybersecurity. [n.d.]. Citizen Clinic. https://cltc.berkeley.edu/citizen-clinic/.

[35] John C Fortney, Jeffrey M Pyne, Eric E Turner, Kellee M Farris, Tre M Normoyle, Marc D Avery, Donald M Hilty, and Jürgen Unützer. 2015. Telepsychiatry integration of mental health services into rural primary care settings. *International Review of Psychiatry* 27, 6 (2015), 525–539.

[36] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[37] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW)* Vol. 1, No. 2 (2017), Article 46.

[38] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[39] Lee Ann Fujii. 2017. *Interviewing in social science research: A relational approach.* Routledge.

[40] Ryan Gabrielson, R. Grochowski Jones, and Eric Sagara. 2014. Deadly Force, in Black and White: A Pro Publica analysis of killings by police shows outsize risk for young black males. *ProPublica: Journalism in the Public Interest* (2014).

[41] Aakash Gautam, Deborah Tatar, and Steve Harrison. 2019. Adding Voices to Support Web Navigation Among a Low Digital Literacy Group. In *Companion Publication of the 2019 on Designing Interactive Systems Conference 2019 Companion*. 165–169.

[42] Liza H Gold. 2020. Domestic Violence, Firearms, and Mass Shootings. *The journal of the American Academy of Psychiatry and the Law* 48, 1 (2020), 35–42.

[43] Diarmaid Harkin. 2019. Regulating private sector security provision for victims of domestic violence. *Theoretical criminology* 23, 3 (2019), 415–432.

[44] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical computer security for victims of intimate partner violence. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 105–122.

[45] Leigh Honeywell. 2019. Personal communication.

[46] Kathrine Huntington. 2020. Journalism in the Age of Doxxing. (2020).

[47] Shanti Kulkarni. 2019. Intersectional trauma-informed intimate partner violence (IPV) services: Narrowing the gap between IPV service delivery and survivor needs. *Journal of family violence* 34, 1 (2019), 55–64.

[48] Jorge Larreamendy-Joerns and Gaea Leinhardt. 2006. Going the distance with online education. *Review of educational research* 76, 4 (2006), 567–605.

[49] Karen Levy and Bruce Schneier. 2020. Privacy threats in intimate relationships. *Journal of Cybersecurity* 6, 1 (2020), tyaa006.

[50] Michael Massimi, Jill P Dimond, and Christopher A Le Dantec. 2012. Finding a new normal: the role of technology in life disruptions. In *Proceedings of the acm 2012 conference on computer supported cooperative work*. 719–728.

[51] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2189–2201.

[52] Brendan R McDonald, Robert D Morgan, and Patrick S Metze. 2016. The attorney-client working relationship: A comparison of in-person versus videoconferencing modalities. *Psychology, Public Policy, and Law* 22, 2 (2016), 200.

[53] Diana Nadine Moreira and Mariana Pinto da Costa. 2020. The impact of the Covid-19 pandemic in the precipitation of intimate partner violence. *International journal of law and psychiatry* 71 (2020), 101606.

[54] J Andrew Morris and Daniel C Feldman. 1996. The dimensions, antecedents, and consequences of emotional labor. *Academy of management review* 21, 4 (1996), 986–1010.

[55] David T Nguyen and John Canny. 2009. More than face-to-face: empathy effects of video framing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 423–432.

[56] Bureau of Labor Statistics. [n.d.]. Workplace Violence in Healthcare, 2018. https://www.bls.gov/iif/oshwc/cfoi/workplace-violence-healthcare-2018.htm

[57] Vicente Peñarroja, Virginia Orengo, Ana Zornoza, and Ana Hernández. 2013. The effects of virtuality level on task-related collaborative behaviors: The mediating role of team trust. *Computers in Human Behavior* 29, 3 (2013), 967–974.

[58] Sachin R Pendse, Faisal M Lalani, Munmun De Choudhury, Amit Sharma, and Neha Kumar. 2020. " Like Shock Absorbers": Understanding the Human Infrastructures of Technology-Mediated Mental Health Support. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[59] Stephen A Rains, Steven R Brunner, Chelsie Akers, Corey A Pavlich, and Selin Goktas. 2017. Computer-mediated communication (CMC) and social support: Testing the effects of using CMC on support outcomes. *Journal of Social and Personal Relationships* 34, 8 (2017), 1186–1205.

[60] Abhilasha Ravichander and Alan W Black. 2018. An empirical study of self-disclosure in spoken dialogue systems. In *Proceedings of the 19th Annual SIGdial Meeting on Discourse and Dialogue*. 253–263.

[61] Rosalie J Russo-Gleicher. 2014. Improving student retention in online college classes: Qualitative insights from faculty. *Journal of College Student Retention: Research, Theory & Practice* 16, 2 (2014), 239–260.

[62] Phoebe Sengers, John McCarthy, and Paul Dourish. 2006. Reflective HCI: Articulating an Agenda for Critical Practice. In *CHI '06 Extended Abstracts on Human Factors in Computing Systems* (Montréal, Québec, Canada) *(CHI EA '06)*. Association for Computing Machinery, New York, NY, USA, 1683–1686. https://doi.org/10.1145/1125451.1125762

[63] Anthony C Smith, Emma Thomas, Centaine L Snoswell, Helen Haydon, Ateev Mehrotra, Jane Clemensen, and Liam J Caffery. 2020. Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19). *Journal of telemedicine and telecare* (2020), 1357633X20916567.

[64] Jessica Soedirgo and Aarie Glas. 2020. Toward Active Reflexivity: Positionality and Practice in the Production of Knowledge. *PS: Political Science & Politics* 53, 3 (2020), 527–531.

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

[66] Geek Squad. 2020. Geek Squad services. https://www.geeksquad.com.

[67] Coalition Against Stalkerware. 2020. Coalition Against Stalkerware. https://stopstalkerware.org/.

[68] Evan Stark. 2009. *Coercive control: The entrapment of women in personal life.* Oxford University Press.

[69] Ronnie J Steinberg. 1999. Emotional labor in job evaluation: Redesigning compensation practices. *The Annals of the American Academy of Political and Social Science* 561, 1 (1999), 143–157.

[70] Jina Suh, Eric Horvitz, Ryen W White, and Tim Althoff. 2020. Population-Scale Study of Human Needs During the COVID-19 Pandemic: Analysis and Implications. *arXiv preprint arXiv:2008.07045* (2020).

[71] Linda Tickle-Degnen and Robert Rosenthal. 1990. The nature of rapport and its nonverbal correlates. *Psychological inquiry* 1, 4 (1990), 285–293.

[72] National Network to End Domestic Violence Safety Net Project. 2020. Response to the COVID-19 Pandemic. https://www.techsafety.org/covid19.

[73] National Network to End Domestic Violence Safety Net Project. 2020. Safety Net Apps. https://www.techsafety.org/safetynetapps.

[74] National Network to End Domestic Violence Safety Net Project. 2020. Technology Safety. https://www.techsafety.org/.

[75] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 1893–1909. https://www.usenix.org/conference/usenixsecurity20/presentation/tseng

[76] Emily Tseng, Fabian Okeke, Madeline Sterling, and Nicola Dell. 2020. " We can learn. Why not?" Designing Technologies to Engender Equity for Home Health Aides. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[77] Jean M Twenge, Brian H Spitzberg, and W Keith Campbell. 2019. Less in-person social interaction with peers among US adolescents in the 21st century and links to loneliness. *Journal of Social and Personal Relationships* 36, 6 (2019), 1892–1913.

[78] Kim Usher, Navjot Bhullar, Joanne Durkin, Naomi Gyamfi, and Debra Jackson. 2020. Family violence and COVID-19: Increased vulnerability and reduced options for support. *International journal of mental health nursing* (2020).

[79] N Van Gelder, A Peterman, A Potts, M O'Donnell, K Thompson, N Shah, and S Oertelt-Prigione. 2020. COVID-19: Reducing the risk of infection might increase the risk of intimate partner violence. *EClinicalMedicine* 21 (2020).

[80] Peter M Vernig. 2016. Telemental Health: Digital disruption and the opportunity to expand care. *Journal of the American Psychiatric Nurses Association* 22, 1 (2016), 73–75.

[81] Douglas M Walls, Brandy Dieterle, and Jennifer Roth Miller. 2018. Safely social: User-centered design and difference feminism. *COMPOSING FEMINIST INTERVENTIONS: ACTIVISM, ENGAGEMENT, PRAXIS* (2018), 391.

[82] John Wihbey and Leighton Walter Kille. 2015. Excessive or reasonable force by police? Research on law enforcement and racial conflict. *Journalist's Resource* (2015).

[83] UN Women. 2020. The COVID-19 shadow pandemic: Domestic violence in the world of work: A call to action for the private sector. https://www.unwomen.org/en/digital-library/publications/2020/06/brief-domestic-violence-in-the-world-of-work.

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

[85] Odette Zero and Meghan Geary. 2020. COVID-19 and Intimate Partner Violence: A Call to Action. *Rhode Island Medical Journal* 103, 5 (2020).

A FOCUS GROUP GUIDES

A.1 General Opinions and Experiences Delivering Remote Consults

(1) Warm-up: Let's go around—how long have you each been doing consults for the remote clinic? Were any of you also part of in-person clinic consults?

Preparing for a consult

(2) How do you prepare for a consult? Can you walk me through an example?
- What are key things you look at in an intake?
- Prior to an appointment, have you ever needed to clarify what comes in on an intake, e.g. the safety assessment or the client's chief concern?
- How would you improve consult prep?

Doing the consult

(3) Without divulging any identifying details, can you tell me the flow of a consult?
- How closely do you adhere to clinic protocols and documents, versus coming up with questions as you go?
- How often do you refer to clinic resources for consultants, like the written guides?

(4) How do you prioritize what to cover in the consult?
- What's your process for interpreting a client's chief concern?
- How do you decide which device or account to check, or what to recommend?
- What makes identifying the client's chief concerns challenging? How do you address those challenges during a consult?
- Without divulging client details, can you provide examples of chief concerns that clients have shared with you?

(5) In your opinion, how often do the client's chief concerns or safety assessment match what is documented in the intake?

(6) What's your experience been with navigating clients through security and privacy settings on their devices via a remote connection?
- What makes this process challenging?
  - How do you address those challenges during a consult?
  - Can you give me an example?

(7) How do you know if the consult is going well, and the client is happy or satisfied?
- Can you give me an example of a time something went well?

(8) Have you participated in a consult in which the client was frustrated or unhappy?
- How did you know?
- Can you give an example? How did you handle it?

(9) How often do you feel like you ran out of time on a consult?
- Why do you think this happens?

Team Communication

(10) How do you and your team communicate before, during, and after a consultation?

(11) What do you typically talk about in pre- and post-meetings?
- How have these been helpful or not helpful?

Post-consult work

(12) After the appointment is finished, what's the flow of wrapping up a consult?
- How much time does post-consult work typically take?
- How much additional research does this usually involve?
- How often do you link clients to guides and other clinic materials?
- Do you think follow-ups are valuable for clients? For case workers?
- How often do you often recommend they come back for another consult?

Wrap-up

(13) In an ideal world, what would you be able to do in a consult that you can't do now?

(14) Is there anything else we didn't ask that you'd like to share?

For senior consultants who approve follow-up emails

(15) What common themes emerge across these post-consult communications?

(16) How do these supplement the remote consults?

(17) Do they extend or match clinic services offered under in-person consults?

(18) What types of issues have you come across that fall outside of the clinic scope?

(19) How often do post-consult communications refer to client concerns that are outside of clinic scope?

A.2 Changes Between In-Person and Remote Consults

(1) Warm up: How long were you participating in the in-person clinic? When did you start doing remote consults?

(2) What do you think are the advantages of a remote clinic compared to an in-person clinic? What has improved?

(3) What has become more challenging in the remote context?

(4) Do you find remote clinic takes more or less work than in-person clinic? Why?

Consult Process

(5) How have your concerns regarding client safety changed from the in-person clinic to the remote clinic?

(6) How have your concerns regarding your own safety changed from the in-person clinic to the remote clinic?

(7) Are you using clinic tools more or less in remote clinic vs. in-person?

(8) A major change from in-person to remote consults is the lack of ability to use a programmatic spyware scanning tool. How has this changed consults?

Interactions with Clients

(9) How have your interactions with the clients changed from in-person to remote clinic?
- Can you give me an example?

(10) How do you feel client experiences or engagement has changed between the remote clinic and in-person?
- What client behaviors lead you to think this?

(11) In your experience, do you generally have more trouble understanding a client's concerns in-person or remote, or is it about the same?

(12) A major difference for remote vs. in-person clinic is that over a remote connection, we cannot see the client's device. How well have your clients understood how to independently navigate their devices for an account or device privacy check?
- Can you think of a time when a client had trouble navigating their device? What kind of issue was it?
- How would you improve this process?

(13) Given that you may not be able to address all of a client's issues, how would you compare the client's experiences with unresolved concerns in remote consultations versus in-person?
- Can you share an example?
- How do you deal with unresolvable issues in remote clinic vs. in-person?

Team Communications

(14) How has team communication changed from in-person to remote?
- Is the level of communication working for you? Do you feel like it's too much or too little?
- Is it hard to keep up with multiple communication channels?

(15) How have these changes in team communication impacted consultations?
- Can you give me an example of how they've improved during the remote clinic?
- Can you give me an example of how team communication presented challenges during the remote clinic?

Wrap-up

(16) Is there anything else you'd like to share that I didn't ask?

A.3 Scheduling and Administrative Work for Remote Consults

(1) Warm-up: Let's go around – how long have you each been doing scheduling for the remote clinic, and which FJCs do you currently handle?
- On average, how many consults do you schedule per week?

(2) Tell me more about the scheduling process. How much work does it take?
- How much back-and-forth is there? Between who?
- How much time does it take?
- What makes it burdensome?

(3) Safety assessment is a core part of the intake process for remote consults. Current protocol states that we ask two questions – whether a client has a safe location and whether they have a safe device.
- Do case workers generally understand what we mean by safe device and safe location?
- Can you tell us about a time you had to follow up after an intake form to get clarification on a client's safety?
- Are there questions you would add or take away?

(4) What happens if a client doesn't have a safe device or location?
- How often would you say this happens?
- Have you had to offer alternative solutions to clients with an unsafe device, e.g. using the conferencing app instead of calling in?
  - Without divulging client details, can you tell us more about that case and how it was handled? What alternatives were offered? Did they work?
- Have you had to offer alternative solutions to clients with an unsafe location?
  - Without divulging client details, can you tell us more about that case and how it was handled? What alternatives were offered? Did they work?

(5) What parts of the intake process do you think work well?

(6) How would you improve the process?

(7) What are your thoughts on moving to direct-to-client scheduling?
- What are the reasons for moving to direct-to-client scheduling?
- What are the benefits?
- What are the challenges?

(8) (If you did intake for in-person consults) What's changed?
- What's been lost and what's been gained in the transition?

(9) Is there anything else you'd like to share?

B CODEBOOK

Theme / Code	Count	**Theme** / Code	Count
Safety issues	**237**	**Access / communication barriers**	**214**
Clients' safety	115	Access to consults	23
Consultants' safety	38	Client didn't have access	12
Breaking anonymity	7	Remote connection difficulties	34
Preserving anonymity	33	Client attendance challenges	26
Unexpected interruption	31	Handling client's emotional dynamic over audio-only	34
Safety planning	9	Client is openly emotional / overwhelmed	37
Limited complementary services	4	Consultant provides reassurance / validation	48
Time issues	**179**	**Spyware / scope issues**	**198**
Prioritization	33	Client story indicates spyware scan needed	27
Not enough time	30	Manual spyware / apps on phone	9
Consultant says clients can schedule another appointment	19	Client wants spyware scan / in-person appointment	5
Reliance on second appointment	7	Unresolved spyware concern	3
Consultant gives client choice	8	Client's concern is out of clinic scope	21
Consultant relies on client to prioritize	4	Challenges managing clients' expectations	25
Narrowing of focus	47	Consultant explains remote clinic limitations	14
Reliance on post-consult communication	31	Client satisfaction	90
		Unresolved concern	4
Remote navigation / new dynamic	**271**	**Confusion / Unfamiliarity**	**124**
Challenges with current tools	13	Client unfamiliar with tech terminology	3
Challenges with lack of visibility	24	Client confusion about technology	22
Challenges with remote navigation	34	Client confusion seems to have resolved	3
Teaching best practices for all technology	20	Consultant gives unclear guidance	9
Teaching best practices for IPV survivors	12	Consultant showing fallibility / saying "I don't know"	30
Remote navigation seems okay	59	On-the-fly research	5
Remote navigation encounters difficulties	37	Consultant will research new topic	16
Consultant as educator	49	Consultant unfamiliarity with specific apps / social media	6
Consultant agency/authority	13	Consultant unfamiliarity with specific platforms	30
Empowering clients	10		
Consultant burdens	**149**	**Consult preparation**	**143**
Clinic takes significant time	32	Preparation case worker communication	49
Disruption to consultants' lives	23	Consult preparation: Reviewing clinic procedures	7
High emotional tax	33	Preparation research	14
High mental overhead	43	Preparation scheduler communication	3
Consultant satisfaction	18	Preparation team coordination	21
		Preparation using own devices	5
		Wish list: More detailed information on clients' situations	44
Consult followup	**34**		
Follow-up case worker communication	2		
Follow-up team coordination / debriefs	7		
Follow-up researching/writing post-consult communications	25		

Table 1: The codebook that resulted from our qualitative analysis, showing themes (bold) and codes, including total count for each theme/code.