Care Infrastructures for Digital Security in Intimate Partner Violence

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

Mehrnaz Sabet
Cornell University
Ithaca, NY, USA
ms3662@cornell.edu

Rosanna Bellini
Cornell University
New York, NY, USA
rfb242@cornell.edu

Harkiran Kaur Sodhi
Cornell Tech
New York, NY, USA
hks59@cornell.edu

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

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

ABSTRACT

Survivors of intimate partner violence (IPV) face complex threats to their digital privacy and security. Prior work has established protocols for directly helping them mitigate these harms; however, there remains a need for flexible and pluralistic systems that can support survivors' long-term needs. This paper describes the design and development of sociotechnical infrastructure that incorporates feminist notions of care to connect IPV survivors experiencing technology abuse with volunteer computer security consultants. We present findings from a mixed methods study that draws on data from an 8-month, real-world deployment, as well as interviews with 7 volunteer technology consultants and 18 IPV professionals. Our findings illuminate emergent challenges in safely and adaptively providing computer security advice as care. We discuss implications of these findings for feminist approaches to computer security and privacy, and provide broader lessons for interventions that aim to directly assist at-risk and marginalized people experiencing digital insecurity.

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, care

ACM Reference Format:
Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3491102.3502038

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3502038

1 INTRODUCTION

While computer security has traditionally focused on protecting information systems, there is increasing recognition of the importance of centering the digital security of people. This perspective on security is most apparent in the growing body of work that aims to understand and improve digital security for vulnerable and at-risk populations, such as political dissidents [30, 43, 45], targets of intimate partner violence (IPV) [26, 27, 48, 75] or online harassment [53], sex workers [4, 62], and journalists [49, 50]. In parallel, scholars have sought to advance frameworks of security as a set of moral obligations, in particular through the feminist *ethic of care* [8, 51, 66]. Viewed through this lens, *care* is the establishment through social and technical infrastructures of ongoing *care relations* that prioritize maintenance of and continual affective attention to others' wellbeing. Care embraces broad consideration for the protection of people, centering collective responsibility and mutuality in the pursuit of fairer and more just sociotechnical systems. A caring approach to computer security and privacy has been considered by Kocksch et al. [41], who re-frame IT security away from the traditional model of (mis)alignment between developers, attackers, and end-users, and towards a notion of security as collective, infrastructural, and care-ful information practice [15, 18, 19].

In this paper, we initiate work on how to practically enact caring infrastructures for security. We do this through an 8-month deployment of an intervention supporting one population particularly in need of computer security assistance: survivors of IPV. Prior work has documented the far-ranging threats to digital security faced in IPV, including the use of spyware (also called stalkerware), abuse of location tracking features, harassment on social media, and more [26, 48, 71, 75]. These threats, termed *tech abuse* in the literature, have invited frameworks for direct interventions helping survivors, including an approach Havron et al. [32] call *clinical computer security*. In this model, volunteer tech consultants met with an IPV survivor in an individualized appointment to address their tech abuse concerns. Prior work has shown this model has been of immediate value to survivors and the broader IPV support community, in both in-person contexts [25] and delivered remotely during COVID-19 [72]—still, there remain a number of open challenges with its one-size-fits-all consultation protocol. As an example, survivors who could not find a safe and private place to take a call were unable to access services. In addition, strict privacy protocols

meant consultants remained completely anonymous, impacting their ability to build trust.

We consider how efforts to evolve clinical computer security for IPV survivors might be enhanced by adopting the ethic of care. Using this framing as a productive lens, we designed a new model for direct security assistance following the principles of care continuity [29], a concept central to professionalized care services in medicine and social work. We describe our new care model, and the social and technical infrastructures we created to enable it. We then report on lessons from our 8-month deployment of it within a computer security clinic operating in partnership with the New York City Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV). Via a mixed-methods analysis of data from 62 client cases, as well as interviews with 18 IPV professionals and 7 volunteer tech consultants, we provide an analysis of the benefits and novel sociotechnical challenges of providing security advice as care infrastructure.

Our findings show that this format of caregiving for computer security required stakeholders to adapt to new challenges around how to safely connect with clients (Section 5.1), how to personalize services for clients' unique needs while maintaining standards of practice (Section 5.2), and how to set appropriate boundaries (Section 5.3). All of this raised further questions around how to define and measure the impact of such services, both within the context of IPV and in security more broadly (Section 5.4). All told, we find that this intervention was necessary and helpful for efforts to support IPV survivors facing digital insecurity, and invites substantial future research drawing ideas from care ethics into how we think about computer security and privacy at the interaction and infrastructure levels. We conclude with reflections on how we might integrate the *"emotional"* and *"technical"* labors of security assistance (Section 6.1), as well as how we might better understand the effects of security interventions centering at-risk or vulnerable people (Section 6.2).

2 RELATED WORK

Working from an empirical basis in computer security and privacy for survivors of IPV (Section 2.1), our paper joins two areas of recent work: research defining *clinical computer security*, a protocol for assisting victims of targeted and persistent privacy threats (Section 2.2); and research within HCI, CSCW and STS examining sociotechnical infrastructures for *care* (Section 2.3).

2.1 The Role of Digital Insecurity in Intimate Partner Violence (IPV)

IPV refers to physical, emotional, verbal, sexual, or economic abuse of a person by a current or former intimate partner. It is a pervasive social problem in the United States of America, in which IPV affects 1 in 4 women and 1 in 10 men [58], including 1 in 2 transgender people [37]. This is in accordance with global estimates that 1 in 3 women have experienced physical and/or sexual violence by an intimate partner, and that an estimated 38% of femicides are committed by former or current intimate partners [59]. Prior work has discussed the role of technology in IPV, through pervasive surveillance and access Dragiewicz et al. call *"digital coercive control"* [20]. Abusers may control victims' devices and accounts, which become conduits for surveillance and harassment even when victims are able to leave [27, 48, 75]. Some harms are levied by installing spyware [13]; however, many are via *"dual-use"* apps: tools built for innocuous purposes that can nevertheless be repurposed for harm by an abuser [26]. Research has also shown how the mere perception of a threat can impact survivors, leading to lack of trust in technology and further isolation from support [46]. Studies also suggest that abusers are enabled by social media, where they receive technical knowledge and narrative justifications for surveillant behaviors [6, 71].

A growing body of research also explores how to aid survivors. Research has highlighted limitations in assessment of tech abuse by existing service structures such as couples therapists [35] and commercial tech support [77]. In response, projects like the National Network to End Domestic Violence's Safety Net [64] and the Coalition Against Stalkerware [61] have created resources for victims, disseminated online and through community-based advocacy organizations. But leveraging resources like these is often challenging for survivors, many of whom are reluctant to engage with technology after their traumatic experiences [27]. Meanwhile, alternative approaches like peer support networks similarly face ethical and practical challenges [7]. Indeed, Kulkarni et al. [42] emphasize that direct resources and services for survivors should center intersectionality and trauma-informed care, via services that consider survivors' specific circumstances and interlocking axes of oppression. Such approaches should also attend to the ways in which offering services can be emotionally arduous for those providing care [12, 14], particularly as organizations are often overwhelmed with demand [5]. To better address survivors' needs, advocacy groups and researchers have developed direct interventions in which survivors meet with technology consultants who assist them with tech abuse. Havron et al. [32] called these approaches *clinical computer security*, drawing on work by Operation Safe Escape [22], the Citizen Clinic [23], and the Electronic Frontier Foundation [24].

2.2 A Technology Clinic for IPV Survivors

Our research took place within a technology clinic (*clinic* hereafter) that was established in late 2018 in New York City to enact clinical computer security and provide IPV survivors with direct help combating tech abuse. The clinic operates within an ecosystem of city-sponsored support services for IPV survivors run by the Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV). Services are coordinated across the city's Family Justice Centers (FJCs), which offer comprehensive support to clients (the term for survivors in this context), including housing, job-seeking, counseling, legal assistance, and more. Among this ecosystem of services, the clinic acts as an authority on technology, specializing in tech abuse. Each FJC assigns a client a specific IPV professional, e.g. a social worker or lawyer, as their primary point of contact (*caseworker* hereafter). Caseworkers handle client referrals to various services, including the clinic. The city operates five FJCs, one in each borough, which in total serve the city's entire population (8.8M as of the 2020 census [52]). Each FJC has its own set of staff and leadership, and the clinic accepts referrals from all five FJCs.

The clinic is staffed by volunteers (*consultants* hereafter) trained in the technical and social aspects of digital security and privacy, as

well as the principles of trauma-informed care. At time of writing, the clinic had approximately 30 consultants, including faculty and graduate students in computer and information science, computer professionals, survivor advocates, and lawyers. To ready them for the challenges of working directly with survivors, each volunteer is equipped to identify symptoms and mitigate aspects of trauma, including vicarious or secondhand trauma. After receiving training delivered by FJC members and other senior clinic consultants, new consultants shadow appointments with more experienced consultants before handling client cases alone. Regular weekly meetings are held between volunteers to discuss cases confidentially, and to provide space for each consultant to reflect on or gut-check their case management decisions. New consultants are also given a private, asynchronous communication channel to reach out to more experienced consultants for well-being support and general advice.

We build on several prior papers that discuss the clinic. Havron et al. [32] describe a protocol in which consultants meet with clients via an individual, in-person appointment to discover and mitigate tech abuse in concert with safety planning by their caseworkers. Freed et al. [25] explored survivor experiences with clinic appointments, analyzing discussions between clients and consultants to identify ethical, sustainability and scalability challenges of intervening. Tseng et al. [72] described how the shift to providing remote appointments during the COVID-19 pandemic required navigating important safety challenges to ensure that remote communication did not put clients or consultants at risk.

Together, these papers provide essential first steps towards understanding how to directly assist IPV survivors with tech abuse; however, they also raise important challenges. First, in prior work, all interactions with clients were strictly **anonymous**: clients and consultants did not know each others' names or any personally identifying information (PII) about each other to increase safety and minimise unnecessary exposure. However, anonymity also resulted in new burdens for consultants, including the need to quickly build rapport with clients without adequate context on clients' needs.

Second, the protocol described in prior papers focuses on a **single hour-long appointment** with a client. Consultants often could not get to all of a client's devices or accounts of concern in one appointment, and scheduling additional sessions required a lengthy back-and-forth with caseworkers [72]. This was because the clinic had no mechanism for enabling the client to meet with same consultants they met with previously. Finally, as a result of the aforementioned safety and time constraints, all client appointments took place **synchronously**, either in-person [32] or remotely [72]. For clients who could not set aside an hour of their day to find a safe and private place for a call, or who were fearful or reluctant to talk on the phone, these appointments were less accessible.

2.3 Creating Caring Infrastructures

To address the aforementioned challenges faced in the clinic, we drew on recent literature advancing the notion that computer security and privacy is less a matter of the shortcomings of a technical system or its users, but rather an ongoing social project of "*collaborative tinkering and experimentation*" spanning multiple sites, scales, and actors—a *matter of care* [41]. This notion of computer security leverages the term *care* to refer to its service-orientation (i.e., the functional provision of necessary services for people, such as healthcare, self-care) *and* its appeal to feminist care ethics [17, 55, 70]. Care is simultaneously practice, such as the continual affective work of attending to one another, and philosophical orientation, towards prioritizing mutual responsibility, concern, and relation with others so that we might "*maintain, continue, and repair our 'world'*" [68]. In this, we follow in the footsteps of many scholars within HCI, CSCW and STS who have embraced care as a framework for analysis in the hope of building sociotechnical systems that are both equitable and responsible [8, 47, 51, 65]. Such works have scrutinized the complex relationships of care and caring between participants and researchers [3, 44], in local communities [38, 74], in organizational practice [74], and in the interactions between people and their devices [40, 66] and their personal data [2, 39].

In work identifying the emotional and intellectual qualities of care inherent to these technosocial interactions, many scholars have grappled with how these relate to systems of labor, and how we build care into systems at scale [67]. If care is to require that we rely on *"momentary orientations and improvisations"* by respecting lived practice and embodied experience [41], standardizing such approaches can be challenging. Berenice Fisher contributes that a core facet of what constitutes care is the notion of performing more than what is required, or to do something '*extra*' [70]. If care always involves something '*extra*', then how might we move care from the status of '*extra*' to '*routine*', for instance in systems for formal caregiving in healthcare, social work—or security and privacy support [41, 69]?

An understanding of security as care also invites examination of how standardized caring behaviors run the risk of transforming ethical and moral relations into those that may cause oppression, inequality and injustice [55, 73]. Consider, for example, the criminal justice system that prosecutes those who cause harm to survivors, and which could be considered an institutional manifestation of caring for survivors' long-term protection [63]. However, for many survivors, progressing through such a system can be a process of re-traumatization in which they must relive accounts of abuse [27]. What's more, subjecting their abusers to incarceration may not ultimately reduce abusive behaviors in the long run. Adopting a *lens of care* for privacy and security for survivors of tech abuse entails that we do not simply understand security as protection from isolated threats such as perpetrators [41, 55], but rather engage with how these threats can stem from a broader insecurity caused by a societal *lack of attention to care* [8] in survivors' lives.

It is through this backdrop that we begin to explore the challenges in standardizing and scaling care for security. To do this, we introduce a model for helping survivors that centers the idea of *care continuity*, a principle in medicine, public health and social work that holds that people seeking formal care (*clients* henceforth, to align with the context of our study) should experience a seamless relationship with the entity providing it. Haggerty et al. [29] defined the concept to consist of three dimensions: *informational continuity*, or the idea that a client's current providers are aware of their prior history and present circumstances; *management continuity*, the idea that the client experiences a "*consistent and coherent*" approach to care responsive to their changing needs, and *relational continuity*, or the idea that an ongoing therapeutic relationship persists between a client and their care providers.

3 PROVIDING LONG-TERM, CONTINUOUS CARE TO SURVIVORS OF TECH ABUSE

To bridge from the anonymous, single-session, and synchronous model of clinical computer security towards a sociotechnical infrastructure capable of providing more flexible, pluralistic, and long-term care, we built a new model to respond to tech abuse that draws on the principles of care continuity outlined by Haggerty et al. [29]. The new model was designed by clinic leadership, in iterative consultation with volunteers, university information technology staff, IRB staff, and ENDGBV leadership. All procedures, including data management systems used, were IRB-approved.

The new model. To overcome the limitations of prior models mentioned in Section 2.2, we designed a new intake and case management process that enables care. Figure 1 depicts the high-level decisions and flow of a client case in the new model. Like previous models, this one was a referral model, where an FJC caseworker determines that a client may benefit from technology support. The caseworker and client fill out an online referral form that gets sent to the clinic administrator, who decides whether the case can be accepted, and if so, which consultant to assign to be the point person. The consultant then contacts the client via the information provided in the referral, and assists through a combination of synchronous phone calls and asynchronous texts and emails. We now highlight how aspects of the new model embody our target care principles of relational, informational, and management continuity.

Relational continuity. Enabling an ongoing therapeutic relationship between a client and their care provider is a key goal of care continuity [29], and more broadly of care as system of commitments and relations. Relational continuity was not possible in the previous model, where clients and consultants remained anonymous to each other and the clinic did not include a mechanism for clients to see the same consultant for multiple appointments.

Realizing this dimension meant creating a tiered model of case management where one specific consultant is assigned to lead all client-facing activities of a specific case—including handling their personally identifiable information (PII). This required a clinic administrator to match clients to consultants, based on a combination of clients' needs and consultants' expertise. (We further detail these matching processes in Section 5.2). To enable each client's consultant to safely reach them while protecting their privacy, we created for each consultant a private email address and a phone number with call and SMS capabilities, neither of which was linked to their real name. This was facilitated via a virtual telephony product contracted by our university and used in other sensitive call centers. Access to these private communication lines was protected by the university's authorization infrastructure, which requires strong passwords and two-factor authentication. These systems afforded relational continuity in the near- and long-term: consultants could safely reach out directly to clients, and clients could reach out to consultants at any time. The boundary negotiations necessitated by these new affordances are discussed further in Section 5.3.

Informational continuity. Haggerty et al. [29] defined informational continuity as the notion that a client's current care providers should have consistent access to details of their prior history and knowledge of their present circumstances. In prior incarnations of clinical computer security, the complete anonymity of the protocol meant consultants walked into appointments with little to no context on a client's situation. Practitioners in healthcare and social services have spent decades enabling informational continuity through case management systems like electronic health records; however, to meet the unique needs of tech abuse survivors, we needed adaptations to meet their stringent safety requirements.

To begin a case, clients and caseworkers work together to submit a referral form that collects details of the client's concerns (e.g., their devices and accounts, along with a general description of the issues they face), alongside their preferred contact method (e.g., phone and/or email), first name, and pronouns. Clients may provide as much or as little information as they like—with the exception of a field asking for contact information for their caseworkers, which was made mandatory to enable safety planning. Figure 2 presents a summary of clients' concerns as represented on the referral forms, including optional demographic information.

Client PII—name, phone number, and email—was made available to *only* the minimum number of clinic volunteers necessary and stored in the fewest systems possible. With respect to the former, both the PII and non-PII information on the form was sent to the clinic administrator, who sometimes assigned cases based on whether contact information was available (e.g., assigning phone-only clients to consultants comfortable with the medium). The assigned consultant then received the PII as part of their notification that they had received a new case. Consultants were instructed to handle PII carefully, and in particular never store it on separate systems or accounts.

The rest of the data on the forms—containing non-PII data on clients' concerns—were stored in a separate and access-controlled cloud storage system used by our university for similarly sensitive data. The cloud storage system allowed joint editing of text documents and was used as a content management system (CMS). Data stored in this CMS consisted of the initial referral details alongside written records of clients' interactions with the clinic (*case notes* hereafter). Written by consultants, case notes consist of semi-structured text files where consultants log clients' concerns as expressed in each appointment, the actions a client has taken, and the status of the case going forward.

Case notes for a client were initially available only to the consultant leading the case. This lead consultant was further granted the option to share the client's folder with additional consultants enlisted to provide specialized advice, so that they could review notes from the client's previous interactions before each appointment. Thus, we enabled informational continuity for both the consultant leading the case, who might go weeks or months between interactions with a client, and for whole consultant teams, in which specialists brought on for specific concerns need a way to get up to speed on the case.

We secured both the PII storage and the CMS systems according to best-practice minimal access policies, and via access monitoring conducted by clinic administration and our institution's data management teams. Client PII was accessible only to the consultant leading a client's case and the clinic administrators. Case notes in the CMS were strictly anonymized and regularly checked by clinic administrators to ensure no PII was stored in those systems. Access

Figure 1: Flowchart depicting the lifecycle of a client's case, including the major entities involved, decisions made, and actions.

to both systems required a two-factor authentication protocol managed by our institution. All data security practices were approved by our institutional IRB.

Management continuity. Lastly, Haggerty et al. [29] reference continuity in management, which aims for clients to experience "*consistent and coherent*" care that is nevertheless still responsive to their changing needs. Consistency in care was achieved through the use of client-facing guides providing best-practice advice on common security problems, which were reported in previous work [72]. To create responsivity towards clients' changing needs, we additionally created flexible communication systems by which consultants and clients could correspond over synchronous or asynchronous lines, e.g. via phone calls, emails, or texts, at whatever cadence made the most sense to them.

The types of advising interactions made possible in the new model are summarized in Figure 1 ("*Consultation*"). In brief, they include (1) holding a synchronous appointment via remote conferencing; (2) corresponding over asynchronous communication lines like email or text; and (3) sharing links to vetted resources, including guides for common security checks either externally produced or developed in-house. With the exception of the synchronous remote appointments, which were developed and described in previous work [32, 72], all these modes of interaction are new to this model. We discuss these interactions further in Section 5.2.

Consistency in care also requires clear messaging on the limitations of a caring entity. As shown in Figure 1, a key consideration for case management was whether the client's needs were a fit for the clinic's services. Clinic staff regularly emphasized with clients and caseworkers that consultants were tech experts, but were not lawyers, mental health counselors, or law enforcement. Clinic administration also emphasized that services were to be delivered remotely, as COVID-19 remained a public health threat in 2021, and, importantly, that consultants were volunteers available by appointment, not on an emergency basis. We discuss the negotiations around these boundaries in Section 5.3.

4 METHODS

To understand how the new model worked in practice, we analyzed data from an eight-month deployment of the model between December 2020 and August 2021. Over the course of our deployment, 107 clients were referred to the clinic. Of these, consultants were able to contact 72 to deliver services, and 62 consented to participate in our research. The clinic continues to offer services to clients at the time of writing. To investigate how the new model was received by various stakeholders, we examined data from (1) real-world cases; (2) interviews with consultants who delivered them; (3) interviews with IPV professionals who refer clients to the clinic. Together, these data reflect reactions to the new model for each of the groups involved, as well as in-depth reflections from consultants and IPV professionals. (We discuss the challenges of eliciting in-depth reflections from clients in Section 6.2). All study procedures were approved by our institutional IRB.

Reflexivity and positionality. Our study embraced a reflexive and autoethnographic form of research, in which researchers' personal biases and experiences are included in the findings [56, 60]. The authors all volunteer in the clinic, where they are part of a larger team of 30+ people, and three authors' experiences as clinic volunteers are represented in the data. In a reflexive study, researchers rotate between subjectivity and objectivity in collaborative sensemaking, creating sites for reflection that enable greater trust and deeper insights than is possible in traditional third-party research.

Clients			
Total research participants	62		
Avg. # devices & accounts	4.34		
Age		Race/Ethnicity	
18–29	5	White	18
30–39	24	Black	13
40–49	18	Latinx	16
50+	15	Other	5
Preferred Pronouns		Preferred languages	
She/her/hers	56	English	54
He/him/his	5	Spanish	9
		Other	4

Client contact	
Phone only	14
Email only	4
Both email & phone safe	42
Neither phone or email safe	2
Devices of Concern	
iPhone	39
iPad	10
Android Phone	16
Android tablet	2
Desktop computer	5
Laptop	35
Other phone	2

Accounts of Concern	
Google	36
iCloud	20
Whatsapp	13
Facebook	26
Instagram	21
Other email	12
Bank account	5
Rideshare accounts	3
Other accounts	17

Figure 2: Client demographics, preferred contact information, and device and account safety concerns, as taken from the referral forms initially submitted by clients. Over the course of our 8-month deployment, $n = 62$ clients consented to participate in our research.

Such methods have been used in prior work to achieve robust understanding of emotionally charged topics [21], and were selected for use here to account for the highly sensitive nature of caring for tech abuse survivors.

As a research group, we are committed to a justice-oriented perspective on security, privacy, and HCI, and aim to support marginalized and vulnerable people through our work. In this, we employ reflexivity throughout to ensure ethical research practice [60]. This paper represents our best efforts to critically appraise our work, in pursuit of lessons for the clinic and for broader efforts in human-centered security and privacy. In the rest of this section, we detail how at each step of our data collection and analysis, we endeavored to create the interplay between researcher subjectivity and objectivity that would produce such appraisals.

Case records. Data from cases consisted of referral forms submitted to the clinic by clients and their caseworkers, written summaries and appointment logs composed by consultants, and professional transcripts of audio recordings of appointments. All participating clients consented to the use of their data for research, and all data were manually scrubbed for personally identifiable details before analysis and reporting. Data from client referral forms, including categorical variables for client demographics and account and device concerns, are summarized in Figure 2.

To more closely examine case progression, the first two authors manually analyzed the 62 written summaries and case logs and identified a diversity of interaction styles (e.g., kind of communication, length of engagement, number of appointments) and concerns addressed (e.g., device and account checkups or additional services sought). To balance subjectivity and objectivity in researcher perspective, these two authors included one whose experiences as a volunteer were represented in the data, and one who had not yet begun seeing clients at the time of data collection. These authors then selected a sample of 12 cases that reflected this diversity for in-depth study.

Then, one author manually reviewed the transcripts of appointments from these cases (~25 total transcripts) and, for each case, developed a set of probing questions for the corresponding consultants. This author was not delivering consults at the time of data collection, and was therefore not a part of the appointments at study. We then reached out to the consultants in this sample (each consultant had 1–3 cases in the sample) and asked if they were willing to participate in an interview. For each consultant who consented to participate, we added case-specific questions to the general interview guide described below.

Interviews with clinic volunteers and IPV professionals. To understand interactions within cases, we conducted semi-structured interviews with clinic volunteers and referring IPV professionals. Interviews were done via 30-minute Zoom calls, which were audio recorded with participants' consent and professionally transcribed.

Our interview subjects included consultants and a clinic administrator in charge of matching clients to consultants. These interviews were led by two authors whose experiences as consultants were not part of the data, and therefore took on the objective role. In total, we interviewed seven volunteers, with levels of experience in the clinic ranging from 12 to 34 months. All had experience in both the previous single-session appointment model and the new care model. Three are authors on this paper. Interviews probed volunteers' experiences with specific clients (identified via the sampling described above), impressions of the new model, and ideas on how they evaluate their work. Appendix A reports the general interview guide used in these sessions, with questions for specific clients redacted to preserve their privacy.

We also interviewed 18 IPV professionals whose clients were referred to the clinic, including caseworkers and leadership at the FJCs and ENDGBV. Since no author is a part of this group, all authors were eligible to take on the interviewing role in these sessions. These interviews inquired after experiences with the new care model, and how stakeholders evaluate the success of support services in their own work (see Appendix A for the interview guide). We recruited a total of seven caseworkers that had referred clients (who consented to participate) to the clinic. We also interviewed ten FJC staff from all five FJCs (1–3 per site), including caseworker supervisors and administrators who manage referrals to partner organizations. Lastly, we interviewed one ENDGBV-level administrator who manages city-wide research and evaluation.

Analysis of our interview data adopted a constructivist thematic analysis approach adapted from grounded theory [10, 11]. We analyzed transcripts by stakeholder group, starting with consultants,

then caseworkers, FJC leadership, and clinic administrator in that order. The first two authors independently coded several transcripts from each stakeholder group, developing separate codebooks for each group. As stated previously, these authors included one whose experiences as a consultant were part of the case data and interviews, and one who was not. (The author who was a subject in the data did not code her own interview.)

These separate codebooks were refined via multiple rounds of reconciliation and consolidated into two codebooks: one for FJC/ENDGBV staff (e.g., *challenges setting boundaries, coordination with support ecosystem, adjustments for clients' tech-savviness*) and another for clinic staff (e.g., *personalized approach, ways of measuring success, handling safety challenges*). The two authors subsequently clustered these codes into one overarching set of themes, which was refined through multiple rounds of iteration with the broader authorship team, including three authors who were interview subjects, and three who were not. We engaged in continuous group reflection throughout the analysis process, employing mutual, verbal sense-making to check our own biases and ensure analysis outputs were appropriately couched as critical reflections. The final themes are reported as Findings in Section 5.

Safety, privacy, and ethics. Throughout our 8-month deployment, we placed great emphasis on ensuring safety and privacy for all participants. Principally, we ensured that participation in research did not interfere with any participant's existing methods of seeking support. Clients' safety was prioritized by making sure their caseworkers were looped in to safety planning, referring them to 911 where necessary, and securing their PII.

We also took extra precautions to respect the safety, privacy and autonomy of our clinic volunteer and IPV professional participants throughout the reflexive interviewing phase of our work. Caring for IPV survivors (particularly amidst a global pandemic) is stressful, and asking care workers to reflect on these experiences can itself be uniquely stress-inducing. We made sure that all interview participants knew they could pause, stop the recording, or decline participation at any point. All participants were assured of anonymity in the reporting of our findings, and we ensured clinic volunteers were interviewed by their peers, not by people who held supervisory roles in their clinic or graduate school work.

Lastly, we took care to preserve participants' safety and privacy in the analysis and reporting of our findings. No identifying information is reported in this paper. Potentially unique phrases have been removed from quotes and stories, and the names of any esoteric tools or apps have been removed.

5 FINDINGS

Our study finds early signals that IPV professionals, clients, and clinic staff appreciate the benefits of a caring approach to computer security and privacy. Clients with shifting and higher-risk security situations are newly able to seek help (Section 5.1), consultants find it enables specialized teams to deliver more targeted assistance (Section 5.2), and caseworkers find it increases clients' confidence in their capacity to secure their profiles and digital devices (Section 5.4). Indeed, IPV professionals and clinic consultants throughout our study were eager to see the clinic grow and serve more clients, from more backgrounds, facing a wider scope of problems. As one member of FJC leadership said:

> *"I think the program is wonderful. It provides a great service to clients to now feel safer, whether in their home, using their device, their email—empowering them to have that ability to take it back and feel safe."* (FJC-01)

Enabling this level of support was not, however, without its challenges—care naturally demands much from the caregiver, hence our strategies put in place to manage volunteer exposure to vicarious trauma and burnout. Our first-of-its-kind implementation of security as care highlights the novel tensions that emerge from creating care relations, and how consultants, caseworkers, and clients adapted to them. We focus on describing clinic *infrastructure*, rather than individual survivor *experiences*, out of the intention to not speak on behalf of clients, who we observed in case data but did not interview. (We detail this tension further in Section 6.2.) As such, we report a limited number of first-person survivor accounts, focusing instead on stakeholders' perspectives on organizational approaches to supporting them. To briefly summarize, we found that consultants and caseworkers worked hard to *safely* reach clients for services (Section 5.1), and to adapt to clients' dynamic and often ambiguous needs (Section 5.2). In doing so, consultants faced constant negotiations around the boundaries of the service and of their availabilities (Section 5.3). Lastly, we found consultants and IPV professionals wrestled with questions around how they could *evaluate* their work supporting clients (Section 5.4).

5.1 Establishing safe connections with clients

A core challenge of this intervention lay in how to ensure that a person facing suspected compromise of their digital devices and accounts could reach out to find support—all while living in a potentially coercive controlling environment. This tension was evident in prior approaches to clinical computer security [26, 72], but was intensified in our new care model, which was designed to enable repeated reach-outs over a longer period of time.

Readiness to engage. We find encouraging signs that the new care model is enabling clients in high-risk safety situations to get help in ways that the previous model might not have afforded. Key to this increased capacity is the *flexibility* to accommodate clients' shifting security situations, e.g., an immediate change in safe contact details or living arrangements. In several cases in our data, clients stop responding for several weeks, prompting a consultant to register their case as inactive and move on—only to hear from the client again weeks later with a call, text, or email letting them know they had managed to find a secure communication line again, and wanted to get help. Enabling this flexibility permitted consultants to handle cases where clients may not be ready to engage with assistance initially, but would be in the future. Reflecting on the new model, one consultant said:

> *"I do think that it does sometimes open [clients] up to more risks depending on their situation, but it also gives them more convenience, and it's about weighing that added risks against the convenience. I'm just really being mindful of respecting their safety needs."* (Consultant-03)

Our analysis finds that in the new model, this *"digital safety dilemma"* was intensified in large part because measures to create relational continuity meant consultants reached out directly to clients, including via cold-calls to initiate their case [72]. The largest challenge, as one FJC leadership participant reflected, was that clients often did not pick up:

> *"There's definitely a lot of cases where you end up playing phone tag. And we learned pretty early on, we had to be very blatant with people. 'We're calling from a private number, pick up that private number. If you're not going to, we get it. But we need another means of communication.' It's been an interesting ride."* (FJC-04)

Clients' reticence to answer the phone was understandable given that they may have experienced harassing phone calls from their abusers—a form of technology-facilitated abuse—requiring consultants and caseworkers to rapidly adapt. As shown in Figure 2, while the majority (42 of 62 clients) did have self-reported safe access to phone or email communication, 18 of 62 reported at time of intake that only one of their phone or email were safe, and two reported that neither line of communication was accessible. Several clients in our dataset provided the contact details of a close friend or family member, and asked the clinic to call at specific days or times.

Offering alternative methods for communication. Using the many affordances of the new care model for protecting client and consultant confidentiality (see Section 3), consultants were able to invest significant effort into ensuring when clients could safely speak, and what modes of communication worked for them. As one consultant described:

> "*I've had clients who were still around their abuser. For them, it's all about making sure we time contact specifically for when [the abuser] is at work or out of the house. I've also had clients who didn't feel safe picking up a call from [our conference line]. It made it really difficult to get things done, because I didn't know that …*" (Consultant-03)

Safety challenges persisted even for clients who did manage to connect with consultants. Anonymity measures in place to protect consultant privacy meant that when a consultant called a client, they would have to greet them, identify themselves and confirm they were speaking to the client—while giving away as few details as possible in case their abuser was listening. Per the new care model, most consultants were intentionally vague in their initial greetings, e.g., saying they were *"calling from the clinic"* before asking whether someone by the client's first name was available. Several consultants took the extra step of using pseudonyms with clients, to protect their own identities.

Consultants agreed the safety constraints of these calls could often create confusion if clients could not realize who they were, or did not immediately remember they had been referred to the clinic. And as one consultant reflected, there was often no good way to do this without referencing security in some way, which could itself retraumatize clients:

> *"Just getting a call from a stranger, saying, 'we're calling from a tech security clinic', they might be taken aback. Especially given that they're already suffering, these words can be triggering. "* (Consultant-04)

This authentication problem was particularly pronounced the first time a consultant made contact, but persisted throughout longer-term engagements where consultants might contact a client weeks after an initial reach-out. It was also heightened by clients' understandable hypervigilance (a state of high alertness common to survivors of IPV, many of whom experience trauma-related stress reactions) to potential communication breaches. (We detail examples of hypervigilance further in Section 5.4). In one case in our data, a client asked a consultant to confirm that the consultant had emailed them weeks before. The consultant had sent a response at an off-hour, using a different greeting and signature than usual, and this deviation in their written communication had made the client concerned someone else (e.g., their abuser) had taken over the consultant's account. Ultimately, the consultant reassured the client verbally on a phone call that it was indeed them who had sent the email, and the case was able to proceed as normal.

Lastly, all of these safety challenges were further complicated by the pressure clients faced to change their contact details. Doing so can be considered best practice for survivors of tech abuse, but it also meant that phone numbers and/or email addresses could change quickly over the course of a client's engagement with the clinic. Such actions made it complicated for consultants to maintain consistent conversations with clients across their multiple accounts.

5.2 Adapting to clients' diverse and changing needs

Another major design goal of our caregiving infrastructure was the ability to specialize the services offered to a client for their unique situation. Our new model allowed for more explicit matching of consultants to cases, and for more personalized plans for clients, through the use of referral forms and case record systems.

Matching client needs with consultant expertise. Our analysis shows the system was successful in enabling clinic administrators to match particularly specialized cases to consultants who could handle them. Most clients sought help for straightforward concerns, for example the security of a Google or Facebook account, which any consultant could take on. In what the clinic administrator estimated as 20–25% of cases, however, clients required more specialized assistance, defined by not only their technical needs (e.g., a more specialized concern like WiFi compromise) but also by their level of risk. Reflecting on how they assigned consultants to clients, the clinic administrator explained:

> *"Technical expertise is only one part of it. Some people might have high technical expertise, but low experience with clients. Other people might have a lot of experience working with survivors, but don't feel very confident about the technical capabilities a certain case needs. I consider an all-rounded picture of expertise ... and for high-risk cases, I try and assign people who have experience and are comfortable with high-risk clients."* (Clinic-Admin)

Assigning cases to consultants based on an "*all-rounded picture of expertise*" helped the clinic provide a flexible service capable of accounting for clients' situated and intersectional needs as expressed in their referral forms. However, consultants explained that often in initial interviews, a different set of problems emerged than

what had been evident at the time of the referral, a misalignment consistent with prior work [25]. As one consultant described:

> *"[The client] always selects a ton of things, like Facebook, Instagram, but then when we ask about their concerns, it doesn't usually include a lot of the things they said. I'm not sure what the disconnect is there."* (Consultant-03)

Reflecting on this factor, consultants in our study described it was frustrating, as they wanted to provide the right kind of support upfront. Many consultants did considerable preparation before each session, for example research to refresh their understanding of particular platforms or tools, only to be directed by the client towards an area that they had not prepared for. Still, many consultants said these mismatches were a natural consequence of the complexity of clients' changing situations, and the need to reduce traumas throughout clients' experiences of care by not asking them to exhaustively detail their experiences at every step. To respect clients' concerns, consultants were trained to take the intake form at face value, but were given the option to request that consultants with different expertise be added to the case if needed.

Building rapport over time. To adapt, consultants used the information on referral forms to prepare ahead of time, but also kept their conversations open-ended and investigational, should new concerns emerge. Importantly, consultants described the care model newly enabled them to build rapport over multiple interactions with clients, in ways that helped them reassure clients and assess concerns over the longer term. For one consultant with a long-running case, the mix of asynchronous and synchronous interactions helped to create a quasi-therapeutic relationship:

> *"A huge amount of the interaction has been [the client] sending me notes every couple of weeks because something new happens, there's some new suspicion. I say some words of reassurance and offer an appointment, and then it's a couple more weeks before she's able to reach back out. Then, when we can talk, she describes something, and I affirm, 'Oh, I remember that happening too. You told me about it.' "* (Consultant-05)

Building this rapport through the new system had clear benefits for clients and consultants, but it also required consultants to deal with inefficiencies to protect clients' privacy. Longer-term cases like this often required consultants to link new incoming messages to old clients, who as described previously may have been reaching out from a different phone or email since the last time they were able to get in touch. In order to provide these clients with relational and informational continuity, consultants had to take the extra step of independently linking new reach-outs to client PII. Consultants also described they took more detailed notes in the case record system specifically to help themselves and others recall important details of clients' cases, should they reach out months in the future.

In addition to enabling consultants and clients to build longer-term rapport, we found that for some clients, the new model had the benefit of encouraging them to seek their own personalized mix of educational resources. Several clients in our study told consultants they had first availed themselves of online privacy guides, including those produced by the clinic, before reaching out to clinic services for a second opinion. As one explained:

> *"I went through the protocol sheets that your organization has, and I changed passwords and updated things. But for maintenance purposes, and as new things have happened, I haven't really had a resource, or someone to bounce things off of, to make sure that everything—even down to our cable modem—is secure."* (Client-30)

Lastly, consultants described they adapted to clients' changing needs through a key new affordance: the ability to bring in additional consultants as needed, to handle new and emerging issues. Consultants described pulling in other consultants for advice on different devices (e.g., an iPhone user asking an Android user for assistance), to work with clients who were more comfortable in different languages (e.g., an English-speaker asking a Spanish-speaker for help), and to address particularly high-risk clients (e.g., a less experienced consultant pulling in a consultant with more experience in trauma-informed counseling). Assembling custom consult teams also helped consultants spread the emotional labor of serving in a quasi-therapeutic role for an IPV survivor (discussed further in Section 6.1). As one consultant in our study reflected: *"For a particularly emotionally heavy case, it's nice to be able to share that with somebody and not have that just on your shoulders."* (Consultant-06). This quote exemplifies that sharing heavier cases with other consultants enabled tacit expressions of care through knowledge-sharing and coaching of best practice, while simultaneously validating a consultants need to process their emotions that may be difficult to make sense of independently.

5.3 Establishing boundaries over time

The new care model did have many positive benefits, in enabling the safer connections and more adaptive services we have described in the last two sections. However, our analysis found delivering security as care also required consultants to *set boundaries with clients*, on the scope of clinic services and on their own availability. These concerns were exacerbated by what consultants described as a lack of clear endpoints in tech abuse cases: fundamentally, our consultants said, it was difficult to know when they had done as best as they could, and step away from the case.

Staying within the clinic's scope. Our data show clients often asked consultants for specific forms of assistance that strained the clinic's scope. Clinic volunteers made every effort to be clear with FJC partners that clinic services included remote assistance with digital privacy and security, for example by investigating clients' devices for spyware or privacy misconfigurations leading to abuse—and did *not* include, e.g., coming to their homes to scan for hidden cameras or listening devices (which would raise significant safety concerns). One consultant described these misunderstandings were often frustrating for them in their role trying to help: *"I feel like I let them down. I do feel we did everything we could, but it's just not in line with what the client wishes would happen"* (Consultant-03).

Another common misunderstanding involved clients asking consultants to help assemble proof of their abusers' actions, often by finding evidence of intrusion on their devices, routers, or accounts. Some of these clients had done research online and found blogs or articles describing how to find such proof, e.g., using network traffic traces sourced via tools like Wireshark. Such requests stretched the technical capabilities of the clinic: intrusions are inherently difficult

to assess remotely, and volunteers did not have the forensic tools or training to handle the ambiguities of, e.g., browsing a router's log of IP addresses to determine which might be cause for concern. More fundamentally, forensic activities involve legal interpretation about evidentiary value for particular statutes. Consultants were always clear these services were outside of the clinic's scope and better addressed by legal counsel, such as a district attorney. Still, clients often sought this form of assistance as part of their efforts to win orders of protection, and other legal matters.

The expectation to be *"always on".* Consultants in our study also reported challenges in setting boundaries around their availability to clients. The many new methods of communication available in the care model had the effect of creating the illusion and expectation that consultants were *"always on"*, one said. The pressure of continuous availability, worsened by the remote and asynchronous nature of the work, created new burdens for consultants: many described responding to emails or texts at odd hours, or sporadically during the day at their full-time jobs, out of an obligation to quickly attend to clients. For one consultant, this pressure sharply contrasted the previous model of single appointments:

> *"Because clients can reach back out to me in theory anytime, I have to respond to them pretty quickly. I think [before this model] it was very easy to feel like, 'My job is just to show up to this for this one hour, and then send an email, and then I'll never have to think about this again.' Now that it's my problem for the foreseeable future, it takes up a lot more time ... It feels like more responsibility."* (Consultant-05)

The pressure to monitor and respond to many lines of communication was heightened in situations where clients reached out with a self-identified emergency. The clinic is not an emergency service, and makes clear to FJCs and clients that they should call 911 or their caseworkers in those situations. Still, our data show establishing this boundary was a source of tension for consultants. One consultant reported that on two separate occasions, clients had reached out to them through emails or texts with messages that suggested they might be immediately unsafe. In both occasions, the consultant was able to respond right away to clarify the client's situation, and instruct them to seek immediate help. However, reflecting on these incidents, the consultant was unsure how to handle future incidents when they might not happen to be available. We discuss the implications of this finding on consultants' roles further in Section 6.1.

Finding the *"sweet spot".* Our analysis found that difficulties around boundary-setting for the scope of clinic services and for consultants' availabilities were exacerbated by a fundamental problem all consultants agreed they faced: how to know when to *stop* providing services. As described by our clinic administration participant, the clinic naturally needed consultants to cycle through cases in order to take on new ones:

> *"Probably the biggest challenge for me is actually trying to get our consultants to try and deal with cases in a reasonable timeframe, or keep the pipeline moving, because [a consultant] having one client for four months means that we're not helping another 10 people."* (Clinic-Admin)

The challenge, this participant elaborated, was to find the *"sweet spot"* where a consultant could support a survivor in higher-touch and longer-term ways—without such engagement becoming unsustainable for the consultant individually and the clinic as a whole. This was easily done in many cases in our data where clients sought help for a fixed question, e.g., whether their abuser had access to a particular email account. In these cases, consultants were able to see the client for an appointment lasting approximately one hour, provide additional resources asynchronously if needed, leave them with the clinic's contact information for the future, and move on.

But in several cases, clients sought *"as much help as possible"*, requesting additional appointments and sending texts and emails with additional questions. Out of a desire to help, consultants sometimes ended up working with them over many appointments stretching on for weeks or months. Reflecting on this time investment, one consultant said:

> *"[The clinic administrator] once told me, 'We cannot be like personal assistants.' But sometimes, based on the first appointment with the client, I feel this person is not very tech-savvy—they do really need some help. So then I end up accepting more and more calls."* (Consultant-01)

As seen in this quote, consultants often struggled to balance becoming *"personal assistants"* for clients' ongoing technical questions, a problem worsened by some clients' relative unfamiliarity with technology, against the broad goal of continuously being available for tech abuse concerns. In many of these cases, working with a client over many appointments was not a *de facto* problem but rather a natural consequence of progression in their tech abuse needs: for example, several cases in our data show consultants checking in with clients over several weeks to guide them through reporting abusive content to social media platforms, a process that by definition takes time.

Difficulties finding natural endpoints. Other cases extended because they began to involve forms of assistance that simply did not have a natural endpoint. Notably, in several cases in our data, consultants struggle to end engagements when it becomes clear that clients' primary needs are further in the realm of emotional support than what consultants are comfortable providing. Reflecting on this dynamic, one consultant described:

> *"I've definitely had a few clients that want to have more appointments, and I get the sense the client just wants to talk. They are scared about the technology stuff, but they want to chat. I've been trying to politely set up boundaries, because I don't know what to do in terms of helping further. It definitely takes up time."* (Consultant-02)

Clinic services explicitly did not include psychotherapy or mental health counseling, for which consultants referred back to clients' caseworkers. But consultants in our study reflected it was often difficult to find the line between tech abuse concerns and concerns that should be routed to a qualified mental health professional. Many interactions within the clinic involved reassuring clients, validating their worries, and providing general psychosocial support, in concordance with the principles of trauma-informed care—but within the new care model, consultants described this form of service began taking up more and more time relative to privacy checks

and security analyses. We discuss the implications of this finding further in Section 6.1.

Ultimately, whether due to clients' needs for more technical or emotional support, or guidance on protracted reporting processes with tech companies, consultants often found it difficult to reach "*resolution*" on a case. As one said:

> *"It's kind of hard to tell when things are going to be at a fixed point. I think in most of my cases, we don't actually resolve the issues in any fundamentally 'we're done' kind of way."* (Consultant-02)

Consultants in our study reflected that this fundamental tension also had immediate consequences for a related problem: how they *evaluated* clinic services, clients' needs, and their own work.

5.4 Looking back on evaluating care

Questions of *evaluation* reverberated throughout our study, as caseworkers, consultants, and other stakeholders reflected on how they could best help clients. The model of providing continuous and longer-term care to clients brought out the need to balance between the many possible outcomes one might aim for when helping survivors overcome tech abuse, and particularly how to measure outcomes within this at-risk population.

Definitions of positive outcomes, and a lack of *"ground truth"*. A core difficulty of security-as-care lay in the uncertainties inherent in securing digital devices for IPV survivors, a finding concordant with previous work [25, 72]. As described in Section 5.3, some clients came to the clinic with straightforward concerns within the clinic's scope, e.g. a request for help walking through the privacy settings on a particular platform or device. But many expressed they did not know what they needed—just that they wanted to feel safe and secure. As one client explained to their consultant:

> *"I guess I'm paranoid about everything, I don't know. But at this point, I don't know what he's capable of doing. I don't know what he's not capable of doing. ... I just want to feel comfortable and confident, moving forward, that my privacy has not been tampered with in any way. I just want peace of mind."* (Client-41)

Helping clients achieve this *"peace of mind"* was difficult for consultants on both a technical and interpersonal level. Clinic investigations used best practices in digital privacy, delivered to the best of consultants' ability, and in many cases, these protocols were able to surface problems that could be leading to the identified compromise. But consultants were often troubled by the fundamental inscrutability of clients' security postures. As one described:

> *"We often don't get any tangible ground truth on what we might've missed. And we don't get feedback often later on ... where they're like, oh, this led to some harm that actually happened for the clients. So it can be very ambiguous."* (Consultant-02)

The lack of *"ground truth"* meant consultants had to carefully navigate how to communicate both positive results, in which clinic investigations turned up identifiable compromise, and negative results, in which clinic checkups did not find any evidence of abuse. In both circumstances, consultants had to relay explanations for this lack of visual indicators of technology abuse through the client's devices or profiles. For example, consultants suggested an abuser may have accessed a client's account through another mechanism, or that all traces of an intrusion were likely lost by the time the client sought assistance (e.g., due to resetting a device). The new care model exacerbated these uncertainties, consultants reflected, because they now dealt with cases that could also change over the length of a client's engagement.

The ambiguous and dynamic landscape of clients' concerns were further complicated by what several consultants described as *hypervigilance*, or the tendency of survivors to remain highly on-alert at all times. Recognized in the clinic's trauma-informed approach to care as a key stress reaction in IPV survivors, hypervigilance manifested in the tech abuse context as continuing suspicion of their devices' every behaviors. As an example, in several cases in our study, a client asks a consultant to check the security of a brand new phone to which the abuser, to their knowledge, has never had physical access, because it has recently dropped some calls.

When working with hypervigilant clients, consultants had to navigate how to accurately communicate the uncertainties inherent to security, while being reassuring. For example, a consultant might explain that most phones are known to occasionally drop calls, and a brand new phone is *highly unlikely* to have been compromised by an abuser who no longer has physical access—but with the appropriate caveat that their situation might be unique. Consultants pointed out that the new care model was actually uniquely beneficial for cases where clients might be hypervigilant: the longer-term rapport made possible by this model gave consultants more opportunities to provide nuanced risk assessments and proactive advice on future best practices. We unpack this tension further in Section 6.1.

The ever-changing ambiguity around whether clients' security postures *could* be accurately assessed meant consultants often focused their efforts on other elements of service delivery more under their control. Several said they were often preoccupied by immediate concerns like whether they could connect to a client, and how quickly they could respond to a client's calls, emails and texts. Consultants reflected this was a natural part of service work, a sentiment echoed by the caseworkers in our study. However, all parties acknowledged it could often be frustrating, as they could not control whether clients ultimately availed themselves of services:

> *"Have I done my part, basically, have I put the ball back in their court? I can't control whether this client actually has an appointment, but I can write back to them whenever they reach out."* (Consultant-05)

More fundamentally, consultants and caseworkers in our study reflected they aimed for a general notion of *empowering* clients in their work. Notions of empowerment are key to the healing and recovery of IPV survivors, per the principles of trauma-informed care. Applicable definitions of empowerment ranged from restoration of a client's locus of control, e.g., "*giving the client that sense of safety again*" (FJC-01), to giving the client tools to handle future problems, e.g., "*they feel like they have more information, they're in the driver's seat*" (FJC-02). For many participants, empowerment for clients also meant demonstrating the extent to which they were supported. As one member of FJC leadership reflected:

> "*I think it can be helpful just knowing that somebody was willing to go that extra mile for them [clients], when they've*

> *never been accustomed to this type of behavior, or service, or support. I think that does make a difference in their way of thinking, and how they manage moving forward. It's like, perhaps they're not ready now, but at least they have the tools and the folks they can reach out to when they are."* (FJC-07)

Empowerment-related outcomes, including those around validating clients' concerns and equipping them to handle future privacy problems, were especially powerful for clients who came in with a baseline low level of *"technical literacy"* (Consultant-06). These clients' concerns could often be addressed by mechanisms like existing privacy controls. Caseworkers felt consultations were especially impactful for these clients. As one said:

> *" After hearing a lot of the things that [the consultant] was helping her with, [the client] was like, 'Oh my god.' It was literally like a setting, and just turning off certain things, like sharing or stuff like that. She felt empowered because she was like, 'Well, I could do this.' "* (Caseworker-07)

For consultants, helping to progress a client's technical literacy was a core positive outcome that, in many cases, developed over the multiple engagements enabled by the new care model. As one consultant said:

> *"It's great to see how they progress—how they start learning new concepts and realizing what is going on with all their tech. [When] we only have one appointment, that progress can't be spotted easily. But when we have more appointments, progress is noticeable, and it's great to see how clients learn from us."* (Consultant-01)

While progress in technical knowledge may have been easy to intuit for this consultant, our study found stakeholders agreed there were numerous other challenges in measuring positive outcomes for clients, which we now describe.

Challenges measuring outcomes with IPV survivors. Given *any* of the aforementioned positive outcomes, how can stakeholders *measure* progress towards these outcomes? According to our participants, getting feedback on clients' progress required overcoming several fundamental challenges in measurement.

First and foremost, consultants, caseworkers, FJC leadership, and clinic administration voiced that clients were by definition *"difficult to reach"*. As previously discussed, clients facing digital insecurity often cannot reliably communicate through digital systems. It follows that survivors who face difficulty even to reach their caseworker may be expected to face difficulty filling out, for example, a feedback survey. FJC leadership described they actually did have a brief satisfaction survey in place—but that it was a city-mandated exercise that did not yield meaningful data, because participation rates were low. Instead, FJC leadership looked to higher-touch forms of feedback like focus groups.

To overcome these challenges, some caseworkers said it might be plausible to have them help clients fill out surveys asking for feedback, the same way they helped clients fill out referral forms. Caseworkers felt this could be a way to not overly burden clients while still enabling their experiences to be known. However, several also reflected that clients may be reluctant to share with their caseworker honest feedback on a service to which their caseworker had referred them.

As another workaround for these measurement challenges, consultants said it may be possible to take a client's verbal feedback during an appointment as a natural signal for satisfaction. However, they were quick to point out that social desirability biases preclude this from being an accurate signal for clients' opinions: clients had a tendency to always thank consultants for their time, regardless of whether they had actually helped. As one consultant said:

> *"You always get thank you. You have to read between the lines to understand how you did. Like from the little cues, how they're responding. Are they confused, or do they have clarity? If they're asking the same thing again and again, they're not getting what you're saying. So you would like, guess from there. But you can't really guess from the end, because at the end of the day, they will always be thankful to you."* (Consultant-04)

As this quote points out, consultants often relied on not on a literal expression of gratitude but more on the client's verbal cues for understanding, e.g., their tone of voice or their words, to signal whether they had successfully reassured them and explained technical concepts. This was often doable in synchronous appointments; however, for asynchronous interactions, consultants said it was often difficult to ensure they were appropriately reassuring clients:

> *"In an in-person appointment, I have a bit of an internal barometer for, do they seem like they believe me? Are they with me? Am I making them feel reassured? Am I conveying confidence? None of those cues exist in an asynchronous conversation. And of course, misunderstandings are very easy over email."* (Consultant-05)

We unpack tensions around defining and measuring outcomes for tech abuse interventions further in section 6.2.

6 DISCUSSION

The development of standardized caring infrastructure for digital security and privacy advice is still in its infancy [67]. Our findings show how our new care model—incorporating a case management system, client-consultant matching, and options for asynchronous communication—enables the *"consistent and coherent"* approach to interventional services that care continuity intends [29]. Accordingly, many of the challenges highlighted, e.g., the need for consultants to set and negotiate boundaries (Section 5.3), can be taken as an indication that the model is establishing care relations, which require ongoing mutual exchange and effort from caregivers.

Addressing these challenges in ways that enable these care relations while lessening burdens on consultants is a fruitful area of future work. In this section, we detail the need for future research in two directions: integrating the *technical* and *emotional* labors involved in security advice (Section 6.1); and measuring security and privacy in at-risk communities (Section 6.2). Within each consideration, we provide lessons for security professionals and researchers around how a lens of care can help us work towards *"rethinking in more fruitful ways how we ought to guide our lives"* [34], towards enabling care infrastructures like the clinic in this study to help more at-risk and vulnerable people facing severe digital insecurity. We close with limitations of the present study (Section 6.3).

6.1 Reconfiguring security towards infrastructural care

Our findings show consultants struggled balancing what may appear at first to be two distinct roles: emotional support and reassurance versus technical computer security advice. Clinic staff were abundantly clear to caseworkers and clients that volunteers were not mental health professionals. Still, many of the interactions in our data resemble interactions one might see in counseling and psychotherapy: rapport-building via demonstrations of empathy and congruence, the encouragement of disclosure and reflection, and the need to set boundaries [36]. In creating the relational continuity that enabled us to support survivors over the long term, we also created conditions for interactions between consultants and clients that take on qualities of a therapeutic attachment. This type of convergence mirrors what Balaam and Hirsch have noted about many types of interpersonal interactions, for example design research: many non-therapeutic interactions can have therapeutic qualities, and in some cases can even have therapeutic effects [3, 36].

The blurring of lines between the *"emotional"* and *"technical"* labors of security assistance is not without discomfort—there certainly exist moments where a client needs specialized and professional mental health services, including where emergency specialists are warranted. However, our findings demonstrate a vast gray area beneath this threshold in which clients seek and receive psychosocial support as a necessary part of support for tech abuse. For example, the interviewing and rapport-building required to elicit enough detail from clients to understand possible sources of compromise are necessarily inflected with empathetic cues and moments of reassurance, and require attention to trauma-informed interviewing techniques so as to not to cause further harm to the client. More subtly, consultants' efforts to provide an *"expert opinion"* on the security of clients' devices and accounts resembles the type of risk assessments and reframings of negative thoughts characteristic of therapeutic approaches in psychodynamic counseling like cognitive behavioral therapy (CBT) [1].

The concordance we observed between security advice and CBT-esque techniques highlights a core difficulty of security-as-care: how can consultants navigate providing security advice in a way that both acknowledges clients' expertise on their own lives and the frequent *"lack of ground truth"* about digital insecurity? Consider, for example, the cases in our study where clients expressed concern that the abuser could hear the calls they made on a brand new phone, one to which the abuser had never had access. The consultants in these situations did the best they could to emphasize that, to the best knowledge available, the risk of compromise was extremely low. But to properly embed care into these interactions, this risk assessment requires not only addressing technical feasibility, but also addressing the clients' knowledge about their situation. Previous results have shown survivor-identified risk of physical or emotional violence is often as accurate or more than standardized risk inventories [16, 33]; the same may be true of technology issues. As such, we consider that security-as-care can be both dyadic and dynamic: a survivor's knowledge can be informed by the consultant carefully providing knowledge of the likelihood and/or possibility of attacks, and a client can likewise inform a consultant of their lived realities with their abuser's unique strategies for causing harm.

That client interactions begin to take on the qualities and difficulties of therapy does not necessarily mean security consultants should shy away from them altogether: volunteers and lay people have always played an important role in the networked schemes of care that constitute "teletherapy", in ways that complement but do not replace professional mental health services [76]. Rather, we view this discomfort as a generative site for future research in clinical computer security, to be done in close collaboration with experts in counseling and psychotherapy. In concert with a shift towards viewing privacy and security as not only a function of the refinement of computer systems but also a function of personal and social data management [19, 41], we need the according attention to how we can standardize these caring practices by integrating what are currently considered two distinct and rarely overlapping skill sets. Doing so might align security as profession more closely with, e.g., teaching and medicine, where natural human instincts to care for one another are not severed in the name of providing expertise. This integration might help emphasize a more global and infrastructural ethic of care, one that encourages the creation of *"more humanly responsive institutions"* that can be curated to include different actors and practices [54]. More broadly, such work might improve computer security research and practice for not only IPV survivors, but also for other vulnerable and at-risk people who stand to benefit from direct computer security assistance, e.g., sex workers, child abuse survivors, and victims of identity theft, to name a few.

6.2 Measuring security outcomes with at-risk communities

Our findings also point to compelling future work negotiating the tensions in evaluation highlighted by our participants (Section 5.4). Security and privacy researchers with quantitative and positivist training, often from computer science, tend to reach for scalable measurements to understand the effect of a given intervention. For example, it is tempting to pursue evidence of impact through individual self-reports solicited from clients (e.g. satisfaction surveys), or population-level econometric assessments of quality of life, with an eye towards generalizing social laws from empirical observation. However, in our work developing and analyzing this intervention, we found challenges with taking this approach at both the philosophical and practical levels: clients are often difficult to reach, as our participants pointed out, and the flexible and personalized nature of tech abuse advice—given by consultants working against security's fundamental *"lack of ground truth"*—make it difficult to imagine an impact assessment for a security intervention that is standardized, fair, *and* valid. What's more, our findings show stakeholders differ in their understandings of what constitute positive or negative outcomes. Clients say they want *"peace of mind"* (5.3), and the knowledge to handle future difficulties. Caseworkers and IPV professionals speak of working towards a sense of *"empowerment"* for clients (5.3), in line with the principles of trauma-informed care, that is often inflected by clients' technical literacy. Consultants, for their part, describe goals around high-quality service delivery (e.g. fast and accurate responses to client reach-outs), and successful communication with clients around realistic assessment of risks.

Drawing on the literature in care ethics [9, 55, 69], we argue these tensions point to a need to foreground interpretive or qualitative notions of assessment when seeking to understand the impact of these interventions. At issue is the core epistemic tension in security as care: where computer security and privacy research is oriented towards measurable outcomes, such a framework may experience tensions with the goals of care relations. Care ethicists have made clear that care has the potential to benefit society at a wider level than being solely confined to the historically feminized private sphere of care work—but when care is formalized in more public spheres, through institutions and social services, it can rub up against existing service infrastructures and their requirements for concrete measurements. Ongoing processes of maintenance and care do not fit neatly into a deterministic and positivist framework of assessment, in which desired outcomes are formalized into proxy variables and measured quantitatively to understand their effect. As an example, when care continuity has been formalized into survey instruments in healthcare settings, it has resulted in scales that effectively count the number of providers a patient sees in the course of a hospital stay [28]. At best, we are reminded that caring behaviors can "fall through the cracks" of being measured [41, 55], and at worst, we are concerned that a preoccupation with quantifiable measurement or datafication can actually impose a lack of care, through a framework that understands care as labor alone [67, 70]. Indeed, ethicists have observed that efforts to standardize and measure care, when not implemented carefully, can inflict the same harm as systems designed to be devoid of it [69, 73].

Yet, the issue remains that if we are to care about caring at a wider scale, we must offer a set of measurements of caring in some way. While stakeholders in our study may have had different interpretations of success, they retained implicit measures of *"good"* or *"bad"* engagements. Further, it is important to teach individuals of the importance of care, even if an individual may be initially reluctant to adopt this view themselves, and it would be challenging to do this without some form of measurement. Practicing caring behaviors can, ideally, lead to the growth of a genuine caring ethic—what begins as a strategic requirement to meet measurable goals can result in genuine care in practice [69]. Notably, though, such calls must be sensitive towards an insincere appearance of caring, or the calcification of caring behaviors into forms of emotional labor as care is professionalized.

As a way forward, we see further research developing ways to evaluate ongoing security care relations *from survivors' perspectives*—after all, our efforts at care are in service to their needs. Crucially, this work must do so in ways that do not re-traumatize them through lengthy or abstract means to gather data. Indeed, the field of HCI has been gradually moving toward the use of qualitative and participatory measurements as indicators of improvement and impact in sensitive contexts such as IPV [3, 7, 57]. This is of acute concern for survivors from marginalized communities, who may be further disadvantaged through such creative approaches if they are used uncritically [31]. We highlight these tensions as lessons for security and privacy researchers intent on doing work that improves conditions for at-risk and marginalized people, and an intriguing point of unification with a growing community in HCI seeking to do the same.

6.3 Limitations

Our study examines problems of security-as-care in one specific context: a clinic for tech abuse survivors in the urban context of New York City, USA, delivered by volunteers with training in the specific security and privacy needs of IPV. Further work is needed to develop additional context-specific insights on how to care for tech abuse survivors in other settings, e.g. in other nationalities and municipalities, in rural or suburban contexts, or in more specific populations (e.g. clinics dedicated to supporting trans survivors). Similarly, our findings do not purport to generalize to security-as-care delivered by other caring systems, e.g. professionals in customer support [77], or by survivors' friends and family. Lastly, our study took a reflexive mixed-methods approach drawing on autoethnography to produce a rich and interpretive picture of how the new care model played out in practice. It is therefore subject to the limitations of all such work: the findings are the product of the authors' lenses. Future work might pursue alternative methods of study, e.g. traditional ethnography by an observer with no first-hand experience in the system at the center of the study, which in conjunction with this paper might triangulate a fuller picture of the phenomenon at hand.

7 CONCLUSION

We discuss a model for providing security advice to at-risk people that incorporates feminist notions of care into an overall sociotechnical infrastructure for caring. We studied this model through an analysis of records from an 8-month deployment in a clinic connecting IPV survivors with volunteer computer security consultants. Our findings show how the approach succeeds in enabling support for survivors with complex and high-risk needs, and invites future work addressing attendant challenges in delivering and assessing security interventions as care infrastructures.

ACKNOWLEDGMENTS

This research was funded by NSF Award #1916096, as well as gifts from Google. ET was additionally supported by a Digital Life Initiative Doctoral Fellowship. 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 all CETA volunteers and staff for their time and commitment to the intervention at the center of this study.

REFERENCES

[1] American Psychological Association. 2017. What is Cognitive Behavioral Therapy? https://www.apa.org/ptsd-guideline/patients-and-families/cognitive-behavioral

[2] Karen S. Baker and Helena Karasti. 2018. Data care and its politics: designing for local collective data management as a neglected thing. In *Proceedings of the 15th Participatory Design Conference: Full Papers - Volume 1 (PDC '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3210586.3210587

[3] Madeline Balaam, Rob Comber, Rachel E. Clarke, Charles Windlin, Anna Ståhl, Kristina Höök, and Geraldine Fitzpatrick. 2019. Emotion Work in Experience-Centered Design. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300832

[4] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. 2021. "Disadvantaged in the American-dominated Internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3411764.3445378

[5] Rosanna Bellini, Angelika Strohmayer, Patrick Olivier, and Clara Crivellaro. 2019. Mapping the margins: Navigating the ecologies of domestic violence service provision. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[6] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. " So-called privacy breeds evil" Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–27.

[7] Rosanna Bellini, Alexander Wilson, and Jan David Smeddinck. 2021. Fragments of the Past: Curating Peer Support with Perpetrators of Domestic Violence. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[8] Cynthia L. Bennett, Daniela K. Rosner, and Alex S. Taylor. 2020. The Care Work of Access. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3313831.3376568

[9] Andrew B.L. Berry, Catherine Lim, Andrea L. Hartzler, Tad Hirsch, Evette Ludman, Edward H. Wagner, and James D. Ralston. 2017. Creating Conditions for Patients' Values to Emerge in Clinical Conversations: Perspectives of Health Care Team Members. In *Proceedings of the 2017 Conference on Designing Interactive Systems (DIS '17)*. Association for Computing Machinery, New York, NY, USA, 1165–1174. https://doi.org/10.1145/3064663.3064669

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

[11] Virginia Braun and Victoria Clarke. 2021. Conceptual and design thinking for thematic analysis. *Qualitative Psychology* (2021).

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

[13] 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.

[14] 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.

[15] Lizzie Coles-Kemp. 2020. Inclusive Security: Digital Security Meets Web Science. *Foundations and Trends® in Web Science* 7, 2 (Dec. 2020), 88–241. https://doi.org/10.1561/1800000030 Publisher: Now Publishers, Inc.

[16] Jennifer K. Connor-Smith, Kris Henning, Stephanie Moore, and Robert Holdford. 2011. Risk Assessments by Female Victims of Intimate Partner Violence: Predictors of Risk Perceptions and Comparison to an Actuarial Measure. *Journal of Interpersonal Violence* 26, 12 (Aug. 2011), 2517–2550. https://doi.org/10.1177/0886260510383024 Publisher: SAGE Publications Inc.

[17] MARÍA PUIG DE LA BELLACASA. 2017. *Matters of Care: Speculative Ethics in More than Human Worlds*. University of Minnesota Press. https://www.jstor.org/stable/10.5749/j.ctt1mmfspt

[18] Paul Dourish and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction* 21, 3 (2006), 319–342.

[19] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[20] Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P Suzor, Delanie Woodlock, and Bridget Harris. 2018. Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies* 18, 4 (2018), 609–625.

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

[22] Operation Safe Escape. 2021. About us. https://safeescape.org/about-us/

[23] UC Berkeley Center for Long-Term Cybersecurity. 2021. Citizen clinic. https://cltc.berkeley.edu/about-us/citizen-clinic/

[24] Electronic Frontier Foundation. [n.d.]. Electronic Frontier Foundation. https://www.eff.org/

[25] 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.

[26] 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.

[27] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–22.

[28] Martin Gulliford, Smriti Naithani, and Myfanwy Morgan. 2006. What is' continuity of care'? *Journal of health services research & policy* 11, 4 (2006), 248–250.

[29] Jeannie L Haggerty, Robert J Reid, George K Freeman, Barbara H Starfield, Carol E Adair, and Rachael McKendry. 2003. Continuity of care: a multidisciplinary review. *Bmj* 327, 7425 (2003), 1219–1221.

[30] Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill, and Ronald J Deibert. 2014. Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware.. In *USENIX Security Symposium*. 527–541.

[31] Christina Harrington, Sheena Erete, and Anne Marie Piper. 2019. Deconstructing Community-Based Collaborative Design: Towards More Equitable Participatory Design Engagements. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 216:1–216:25. https://doi.org/10.1145/3359318

[32] 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.

[33] D. Alex Heckert and Edward W. Gondolf. 2004. Battered Women's Perceptions of Risk Versus Risk Factors and Instruments in Predicting Repeat Reassault. *Journal of Interpersonal Violence* 19, 7 (July 2004), 778–800. https://doi.org/10.1177/0886260504265619 Publisher: SAGE Publications Inc.

[34] Virginia Held. 2005. *The Ethics of Care: Personal, Political, and Global*. Oxford University Press, New York. https://doi.org/10.1093/0195180992.001.0001

[35] Katherine M Hertlein, Brandon P Eddy, and Morgan Lancaster Strickland. 2020. A Framework for Assessing Technology-Mediated IPV. *Journal of Couple & Relationship Therapy* 19, 4 (2020), 296–321.

[36] Tad Hirsch. 2020. Practicing Without a License: Design Research as Psychotherapy. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3313831.3376750

[37] Sandy James, Jody Herman, Susan Rankin, Mara Keisling, Lisa Mottet, and Ma'ayan Anafi. 2016. The report of the 2015 US transgender survey. (2016).

[38] Elizabeth Kaziunas, Michael S. Klinkman, and Mark S. Ackerman. 2019. Precarious Interventions: Designing for Ecologies of Care. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 113:1–113:27. https://doi.org/10.1145/3359215

[39] Elizabeth Kaziunas, Silvia Lindtner, Mark S. Ackerman, and Joyce M. Lee. 2018. Lived Data: Tinkering With Bodies, Code, and Care Work. *Human–Computer Interaction* 33, 1 (Jan. 2018), 49–92. https://doi.org/10.1080/07370024.2017.1307749 Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/07370024.2017.1307749.

[40] Cayla Key, Fiona Browne, Nick Taylor, and Jon Rogers. 2021. Proceed with Care: Reimagining Home IoT Through a Care Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.

[41] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT security: Accountabilities, moralities, and oscillations in IT security practices. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[42] 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.

[43] Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda. 2014. A Look at Targeted Attacks Through the Lens of an NGO. In *USENIX Security Symposium*. 543–558.

[44] Ann Light and Yoko Akama. 2014. Structuring future social relations: the politics of care in participatory practice. In *Proceedings of the 13th Participatory Design Conference: Research Papers - Volume 1 (PDC '14)*. Association for Computing Machinery, New York, NY, USA, 151–160. https://doi.org/10.1145/2661435.2661438

[45] William R Marczak, John Scott-Railton, Morgan Marquis-Boire, and Vern Paxson. 2014. When Governments Hack Opponents: A Look at Actors and Technology.. In *USENIX Security Symposium*. 511–525.

[46] 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.

[47] Shannon Mattern. 2018. Maintenance and Care. *Places Journal* (Nov. 2018). https://doi.org/10.22269/181120

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

[49] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. 2015. Investigating the Computer Security Practices and Needs of Journalists. 399–414. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/mcgregor

[50] Susan E. McGregor, Elizabeth Anne Watkins, Mahdi Nasrullah Al-Ameen, Kelly Caine, and Franziska Roesner. 2017. When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. 505–522. https://www.usenix.

org/conference/usenixsecurity17/technical-sessions/presentation/mcgregor
[51] Amanda Meng, Carl DiSalvo, and Ellen Zegura. 2019. Collaborative Data Work Towards a Caring Democracy. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 42:1–42:23. https://doi.org/10.1145/3359144
[52] NYC Department of City Planning. [n.d.]. Population of New York City. https://www1.nyc.gov/site/planning/planning-level/nyc-population/nyc-population.page
[53] Jeremiah Onaolapo, Nektarios Leontiadis, Despoina Magka, and Gianluca Stringhini. 2021. SocialHEISTing: Understanding Stolen Facebook Accounts. 4115–4132. https://www.usenix.org/conference/usenixsecurity21/presentation/onaolapo
[54] Fiona Robinson. 1997. Globalizing Care: Ethics, Feminist Theory, and International Relations. *Alternatives: Global, Local, Political* 22, 1 (1997), 113–133. https://www.jstor.org/stable/40644882 Publisher: Sage Publications, Inc.
[55] Fiona Robinson. 2011. *The Ethics of Care: A Feminist Approach to Human Security*. Temple University Press. https://www.jstor.org/stable/j.ctt14bt8bq
[56] 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
[57] Julia Slupska and Leonie Maria Tanczer. 2021. Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited.
[58] Sharon G Smith, Xinjian Zhang, Kathleen C Basile, Melissa T Merrick, Jing Wang, Marcie-jo Kresnow, and Jieru Chen. 2018. The national intimate partner and sexual violence survey: 2015 data brief–updated release. (2018).
[59] Social Determinants of Health. 2014. *Global status report on violence prevention*. Technical Report. World Health Organisation. 1–274 pages. https://www.who.int/publications-detail-redirect/9789241564793
[60] 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.
[61] Coalition Against Stalkerware. [n.d.]. Coalition Against Stalkerware. https://stopstalkerware.org/
[62] Angelika Strohmayer, Jenn Clamen, and Mary Laing. 2019. Technologies for Social Justice: Lessons from Sex Workers on the Front Lines. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300882
[63] Anna Terwiel. 2020. What Is Carceral Feminism? *Political Theory* 48, 4 (Aug. 2020), 421–442. https://doi.org/10.1177/0090591719889946 Publisher: SAGE Publications Inc.
[64] National Network to End Domestic Violence. [n.d.]. Safety Net Project. https://nnedv.org/content/technology-safety/
[65] Austin Toombs, Laura Devendorf, Patrick Shih, Elizabeth Kaziunas, David Nemer, Helena Mentis, and Laura Forlano. 2018. Sociotechnical Systems of Care. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '18)*. Association for Computing Machinery, New York, NY, USA, 479–485. https://doi.org/10.1145/3272973.3273010
[66] Austin L. Toombs, Shaowen Bardzell, and Jeffrey Bardzell. 2015. The Proper Care and Feeding of Hackerspaces: Care Ethics and Cultures of Making. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 629–638. https://doi.org/10.1145/2702123.2702522
[67] A. L. Toombs, A. Dow, J. Vines, B. Dennis, R. Clarke, A. Light, and C. M. Gray. 2018. Workshop proposal: Designing for everyday care in communities. *DIS 2018 - Companion Publication of the 2018 Designing Interactive Systems Conference* (2018). https://doi.org/10.1145/3197391.3197394 Publisher: Newcastle University.
[68] Joan C. Tronto. 1998. An Ethic of Care. *Generations: Journal of the American Society on Aging* 22, 3 (1998), 15–20. https://www.jstor.org/stable/44875693 Publisher: American Society on Aging.
[69] Joan C. Tronto. 2010. Creating Caring Institutions: Politics, Plurality, and Purpose. *Ethics and Social Welfare* 4, 2 (July 2010), 158–171. https://doi.org/10.1080/17496535.2010.484259 Publisher: Routledge _eprint: https://doi.org/10.1080/17496535.2010.484259.
[70] Joan C. Tronto and Berenice Fisher. 1990. Toward a Feminist Theory of Caring. *Circles of Care* (1990), 36–54. https://experts.umn.edu/en/publications/toward-a-feminist-theory-of-caring Publisher: SUNY Press.
[71] 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)*. 1893–1909.
[72] 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 *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.
[73] F. Vera-Gray. 2020. The whole place self : reflecting on the original working practices of rape crisis. *Journal of gender-based violence*. 4, 1 (Feb. 2020), 59–72. https://doi.org/10.1332/239868019X15682997635986 Num Pages: 0 Number: 1 Publisher: Policy Press.
[74] Nervo Verdezoto, Naveen Bagalkot, Syeda Zainab Akbar, Swati Sharma, Nicola Mackintosh, Deirdre Harrington, and Paula Griffiths. 2021. The Invisible Work of Maintenance in Community Health: Challenges and Opportunities for Digital Health to Support Frontline Health Workers in Karnataka, South India. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 91:1–91:31. https://doi.org/10.1145/3449165
[75] Delanie Woodlock. 2017. The abuse of technology in domestic violence and stalking. *Violence against women* 23, 5 (2017), 584–602.
[76] Hannah Zeavin. 2021. *The Distance Cure: A History of Teletherapy*. MIT Press.
[77] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*. 429–446.

A INTERVIEW GUIDES

A.1 Consultants

(1) With the new model, we have introduced several new capabilities: an intake form, reaching out to clients directly for scheduling, the ability to schedule follow-up appointments, and/or conduct our work with clients asynchronously, e.g. via email or text.
   - Has this model been helpful in providing services to clients? Why or why not?
   - What are some of the challenges that you have experienced with this model?
   - What are some of the benefits?

(2) Has this model changed your approach to addressing client concerns? In what ways are the substance of your consults different from pre-DTC?[1]

Intake form

(3) How do you use the information on an intake prior to a consult? During a consult?
(4) Is the intake form helpful for you?
   - In what ways?
   - How could it be improved?

Reaching out to the clients

(5) How do you usually reach out to clients?
(6) How often do you never hear back from clients?
(7) What are some of the challenges that you've faced reaching out to clients to schedule an appointment?
(8) How do you feel about having access to client PII in the new DTC model? How does this affect the way you connect with clients and communicate with them?
   - Do you use your real name with clients? Why or why not?
   - If no, how do you handle the asymmetry this creates, where you know the client's PII but they don't know yours?

Follow-up appointments

(9) Having the ability to schedule follow-ups is a new feature of DTC. How has this ability changed the way you navigate and address clients' concerns?
(10) How often do you find a major issue/suspicious activity during the course of a follow-up session rather than in the first consultation session?
   - Do clients bring up new/different sets of problems during a follow-up session?

Interactions with clients between sessions

(11) How do you manage multiple appointments and streams of communication with clients?
(12) How often do you end up communicating with a client asynchronously, before or after sessions?
   - Without divulging identifying details, can you describe how these conversations tend to go? Are these burdensome for you?
   - How often do clients initiate these interactions?

Measuring Success

(13) How do you think about your success in managing the cases assigned to you?
   - *If consultant worked the pre-DTC model:* Has the new model changed the way you think about "success" in a client case? If so, how?
   - How can you tell when a client is happy or unhappy with the clinic's services?
   - Compared to things you described for scuccess, what does failure look like to you?

(14) Overall, how do you think the clinic should evaluate the impact or success of its services?

Wrap-up

(15) Do you have any suggestions for improving the DTC model?
(16) Is there anything else you'd like to tell us?

A.2 Case Workers

(1) Let's start. Can you tell us about your FJC affiliation?
   - How do you decide to refer a client to CETA?
   - Can you think of any cases of tech abuse that you did not refer to CETA? We're curious to know why not.
   - What challenges does having a client with tech abuse add to your workflow?
   - When you're referring a client, do you fill out our intake form for the client or does the client fill it out themselves?
     - Is the client present when you fill it out?
     - Is there anything on the intake form that is unclear or challenging for you?

(2) Have clients told you about their experiences with CETA, such as after they've had an appointment with us? Yes/No
   - Without divulging specific client details, can you share any examples?
   - Did the client say things that suggested CETA did or did not help them?
   - Can you tell me about a time when a CETA consultation did help your client?
   - Can you tell me about a time when a CETA consultation did not help your client?

(3) In your experience, has meeting with CETA changed clients' tech-related concerns at all?
   - Did they still have significant tech concerns?
   - Did they have new or different concerns as a result of meeting with CETA?

(4) In your opinion, has CETA helped clients feel more or less in control of their technology?
(5) What do you consider to constitute "success" in your work with clients?
   - What is "failure", or less than successful?

(6) How do you think CETA should try to evaluate its work with clients?
   - How do you believe CETA should measure the success of its work?

(7) What suggestions do you have for how we can improve our services?

[1] Within CETA, the new care model described in this work is referred to as Direct-To-Client (DTC).

(8) What suggestions do you have for how we can improve our services for caseworkers like yourself?
(9) Is there anything else you'd like to share?

A.3 FJC Leadership

(1) Let's get started. Can you talk a bit about how you engage with CETA right now?
    - e.g., Do you refer clients to us? Do you handle Norton requests?
(2) How do caseworkers at your FJC learn about CETA's services / referrals?
    - How do caseworkers/clients get an intake link?
(3) How well is the current referral model working for you and your staff?
    - Has it become easier to refer clients to us?
    - Is there extra work on your end or for the caseworkers?
    - What challenges / pain points do you or your staff have with CETA's current model?
(4) Have FJC caseworkers discussed with you their experiences with CETA?
    - Did they feel that CETA did or did not help their clients?
    - Did caseworkers report back on CETA's current model vs. previous referral models?
    - Have they brought up any challenges / pain points that we should know about?
(5) What are your general thoughts on CETA and the services we provide?
    - What suggestions do you have for how we can improve our services?
    - What suggestions do you have for how we can make your life easier as FJC Director?
(6) For the cases handled through your FJC, what does "success" look like? How do you evaluate your work with clients?
    - What might "failure" look like with a client?
    - How do you think CETA should evaluate its work with clients? How can we know if we're actually helping clients?
(7) In addition to your FJC leadership responsibilities, do you presently see clients as well?
    - If so, how many clients have you personally referred to CETA thus far?
    - Do you know if CETA's services made any difference to your clients' situation?
    - Do you have any other relevant feedback on your experiences with clients who met with CETA?
(8) Is there anything else you'd like to share with us that we haven't already covered?

A.4 CETA Administrator

(1) Can you describe the process you go through from the moment you receive an intake form to when you assign it to a consultant?
(2) How do you process (filter) the information on the intake form to decide about who to assign it to?
    - Which parts of the intake form information are most important to you for assigning consultants?
    - Which parts have priority to you when you want to process the information? (e.g. type of devices, number of concerns, etc)
    - Do you also take any consultant preference into consideration when assigning the cases?
        – If yes, does it cause any imbalance in terms of the type of the cases (like for example the mode of communication) that are assigned to consultants?
    - Do you think expertise is more important or seniority for choosing consultants when assigning them to a case? Why?
    - Is expertise the only kind of consultant preference you consider? (e.g. preferred mode of communication, demographics, etc?)
        – Other than technical expertise; what are the non-technical capabilities you consider?
(3) What are some of the challenges that you face for assigning cases?
(4) What do you do when the designated consultant in your mind doesn't have capacity to take a new case?
    - Do you think that's a problem?
(5) How do you compare case management now to pre-DTC? What are some of the benefits and drawbacks of the new model with that regard?
(6) Do you think the case assignment process affects the success of the cases? Why or why not?
(7) How do you evaluate your success in case assignment?
(8) What do you think about the success of the cases overall?
    - How do you follow-up on the outcome of a case and when do you do it?
(9) How do you think CETA should measure the success of its services?
(10) What are some of the main challenges that you think DTC has caused for CETA?
(11) Do you have any suggestions for improving the DTC model?

B CETA VOLUNTEERS CODEBOOK

Theme / Code	**Theme** / Code
New burdens on consultants	**How consultants personalize services**
Case management internal processes	Consultants sensitive to client's trauma
Perceived distance from FJC caseworkers	Consultants sensitive to client's previous help-seeking
Coordination challenges over asynchronous communications	Consultants sensitive to client's tech-savviness
Intake information quality varies	Consultants refer to intake form information
Scheduling remains a challenge	Consultants try to reassure clients
Mismatch between intake and clients' concerns in consult	Consultants assemble custom consult teams
Success indicators	**Sources of variability in success indicators**
Clients' verbal feedback	Client's tech-savviness
Results of security checkup	Client's trauma
Caseworker feedback	Inherent uncertainty of computer security
Consult team feedback	Progression in clients' knowledge
Service delivery	Progression in clients' needs
DTC gives increased flexibility	**Cadence of success measurement**
PII helps with rapport-building	Measuring success over long term
Continuity helps with rapport-building	Some clients don't need regular check-ins
Consultant splits concerns over multiple appointments	Need for regular check-ins with clients
Async communication has benefits	
DTC has coordination benefits	
DTC has increased capacity	
DTC has scheduling benefits	
Handling safety challenges	**Lofty expectations of computer security**
Clients need to authenticate CETA reach-outs	Setting consultants' expectations of clients
PII creates safety challenges	Setting clients' expectations of CETA
Async creates safety challenges	
Challenges reaching caseworkers for safety planning	
Setting boundaries around availability	
"always-on" availability requires boundary-setting	
Consultants feel obligated to keep following up	
DTC allows emergency connection	

Table 1: The codebook that resulted from our thematic analysis of interviews with volunteer consultants (see Appendix A.1 for interview guide) and clinic administration (see Appendix A.4).

C FJC CASEWORKERS & LEADERSHIP CODEBOOK

Theme / Code	**Theme** / Code
Different definitions of success	**Measuring success**
Success as concerns addressed	Clients are hard to reach for follow-up
Success as happier emotional state	Client's survey responses can be biased
Success as empowering client for the future	Existing satisfaction survey isn't used for evaluation
Success as impact in client's life	Caseworkers imagine stepwise success measurement
Success as engagement	Clients volunteer feedback to caseworkers when things go well
Success as progression in client's knowledge	Measuring success via evidence gathering for client
Client-centered approach means success is ad-hoc	Measuring success via service delivery
	Measuring success requires multi-pronged approach
	Measuring success via client's verbal feedback
	Measuring success via focus groups with survivors
	Measuring success by following up with client
Lofty expectations of computer security	**Uncertainty around safety**
Caseworkers and FJCs don't understand tech concerns	Caseworker defers to client for safety of communication line
When in doubt, caseworkers bias towards referring to CETA	Caseworker still needs to coordinate when devices are compromised
Caseworkers don't know what CETA expects from them	Caseworker and FJC filling out intake helps safety and coordination
Criteria for referral to CETA	
Constantly managing client expectations	
Coordination with support ecosystem	**Challenges around boundary-setting**
CETA's role is tech only	Demand for on-call services
Caseworkers want screening for tech abuse upstream	Demand for increased capacity
Caseworker and FJC are connector to other resources	Caseworker serves as crisis support
DTC has coordination benefits	Hybrid method for service delivery would work best
Caseworkers find intake form helpful	Consultants need to persistently follow up with recaps and next steps
Scheduling is improved but still cumbersome	Clients request additional services for new issues
Adjustments for clients' tech-savviness	
Clients don't know how much more CETA can help	
Clients decide they don't want service after all	
CETA is very helpful for less tech-savvy clients	
Less tech-savvy clients need more follow-up	

Table 2: The codebook that resulted from our thematic analysis of interviews with FJC caseworkers (see Appendix A.2 for interview guide) and leadership (see Appendix A.3).