# The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence

Yixin Zou[1] Allison McDonald[1] Julia Narakornpichit[2] Nicola Dell[2] Thomas Ristenpart[2]
Kevin Roundy[3] Florian Schaub[1] Acar Tamersoy[3]
[1] *University of Michigan* [2] *Cornell Tech* [3] *Norton Research Group*

## Abstract

Technology plays an increasingly salient role in facilitating intimate partner violence (IPV). Customer support at computer security companies are receiving cases that involve tech-enabled IPV but might not be well equipped to handle these cases. To assess customer support's existing practices and identify areas for improvement, we conducted five focus groups with professionals who work with IPV survivors ($n$=17). IPV professionals made numerous suggestions, such as using trauma-informed language, avoiding promises to solve problems, and making referrals to resources and support organizations. To evaluate the practicality of these suggestions, we conducted four focus groups with customer support practitioners ($n$=11). Support practitioners expressed interest in training agents for IPV cases, but mentioned challenges in identifying potential survivors and frontline agents' limited capacity to help. We conclude with recommendations for computer security companies to better address tech-enabled IPV through training support agents, tracking the prevalence of these cases, and establishing partnerships with IPV advocates.

## 1 Introduction

Intimate partner violence (IPV) — abuse or aggression that occurs in a romantic relationship — is a pervasive societal phenomenon that causes physical and psychological harms to victims [22]. In the United States, more than one in three women and one in four men have experienced rape, physical violence, and/or stalking by an intimate partner in their lifetime [35]. Research shows that technology plays an increasingly salient role in IPV [28, 53, 70, 85]. In particular, a growing number of mobile apps enable abusers to surreptitiously spy on, harass or impersonate their intimate partners [6, 10, 64, 79].

Providing technical support to survivors of technology-enabled IPV is challenging. IPV professionals such as social workers and lawyers report having insufficient technical expertise [27]. Tools for detecting spyware and other malicious apps still have a high false-negative rate [10]. Resources for IPV professionals and survivors mostly include high-level advice without standardized procedures for flagging and addressing tech issues [27]. The Clinic to End Tech Abuse [77] in New York City and the Technology-Enabled Coercive Control Clinic in Seattle are examples of personalized computer security assistance to IPV survivors, but these services are currently small and only available in specific locations [32].

We take a different perspective by focusing on customer support agents at computer security companies for several reasons. These agents are trained to troubleshoot tech issues, and prior work shows that customers turn to them for a wide range of security issues beyond products [67], making them a likely point of contact for survivors experiencing tech-enabled IPV. Computer security companies offer products that can help survivors by catching spyware or other malicious apps, meaning that the tech help provided by support agents, when contacted by survivors, can be timely and impactful. Additionally, several large computer security companies have expressed interest in supporting IPV survivors, forming the Coalition Against Stalkerware [71]. However, helping IPV survivors through customer support requires extreme care and caution. Inappropriate responses or recommendations might re-traumatize survivors [50] or even escalate violence as abusers seek to regain control [25, 27, 86].

We investigate the opportunities and challenges for computer security customer support to help IPV survivors via three steps:

1. To discover if customer support agents already encounter IPV cases, we searched customer support cases at a large computer security company. Our search surfaced at least 53 tech-enabled IPV cases, in which survivors described the attacks' severity and resulting distress. Support agents typically focused on technical solutions without expressing sufficient empathy or awareness of IPV.
2. Having established that support agents encounter tech-enabled IPV cases, we explore how customer support could better serve IPV survivors by engaging 17 IPV profession-

als from five support organizations in focus groups. IPV professionals provided numerous suggestions, such as using trauma-informed language, avoiding promises to solve problems, and making referrals to external resources for support beyond the immediate technical issue.

3. To gauge the practicality of IPV professionals' recommendations, we conducted focus groups with 11 customer support practitioners from four large computer security companies. Practitioners agreed on the importance of training agents for IPV cases but mentioned implementation challenges, such as frontline agents' limited capacity and uncertainty in identifying whether a customer may need IPV-related help.

Through this process, we thoroughly engaged with multiple stakeholders and synthesized their insights into novel recommendations that both cater to the needs of IPV survivors and consider the real-world constraints of customer support. To better address tech-enabled IPV, we recommend that computer security companies should train support agents to be aware of IPV's prevalence, the limitations of security software in curbing IPV, and when and how to provide additional help. Tracking the frequency and nature of relevant cases would help companies assess their current practices and determine areas to invest in. We further note the opportunity for computer security companies and IPV advocates to learn from each other's expertise and join forces to help IPV survivors combat tech-enabled abuse.

## 2 Background and Related Work

A growing body of literature on tech-enabled IPV has documented the many ways abusers maliciously use technology [25,28,33,45,46,48,49,70,85] and how IPV survivors struggle to protect their privacy and security [17,18,27,53]. The complex socio-technical and legal factors embedded in the intimate relationship differentiate tech-enabled IPV from abuse in other contexts such as online harassment [74], doxxing [69], cyberstalking [25], and cyberbullying [83].

**Malicious apps in IPV.** Tech-enabled IPV often occurs through surveillance apps installed on survivors' devices [10, 27, 31, 47, 53]. mSpy, one of the largest spyware vendors, allegedly had around two million users as of 2014 [13]. In NortonLifeLock's 2020 survey, 10% of respondents admitted using an app to monitor a former or current partner's messages, calls, emails, or photos [78].

Most spyware apps are in fact dual-use, i.e., they have a legitimate purpose (e.g., "Find My Phone" for anti-theft) but can be repurposed for spying on an intimate partner [10]. Growing awareness of the spyware problem has led to improved detection features and related research [11,19,24,64]. Some security companies have joined forces with one another and with IPV advocacy groups through the Coalition Against Stalkerware [71]. Regulators are also strengthening their oversight on spyware, such as the US Federal Trade Commission's settlement with Retina-X in 2019 [72].

**Interventions against tech-enabled IPV.** In addition to spyware detection tools, prior work has proposed apps and operating systems that can help IPV survivors by erasing browser history [20,73], recording evidence of abuse [3], or engaging in safety planning [38]. However, few of them have received wide adoptions among IPV survivors. Support organizations such as NNEDV [76] and Safe Horizon [34] have provided tech-focused resources for survivors, but these resources are often out of date or lack detailed guidance [27]. Computer security clinics are a recent approach for helping IPV survivors through one-on-one consultations with trained technologists, who analyze survivors' digital assets and provide personalized advice on resisting tech-enabled attacks [26,32,80]. Despite early evidence of success, these clinics are currently limited to the serving geographic locations [32] and face numerous challenges in remote operations [80]. Our focus — computer security companies' customer support — has the potential to reach a broad audience, but this approach requires careful attention to the nuances and unique risks in IPV to avoid unintentional harm.

**Customer Support.** Customer support plays a crucial role in helping customers make purchase decisions, providing guidance on product use, and resolving problems or complaints [7]. Reliability, assurance, tangibles, empathy, and responsiveness (RATER) are key metrics in evaluating customer support's quality [61]. Support agents need to make customers feel heard and respected to create a positive customer experience [5]. In particular, past research highlights the importance of training support agents in information technology to use phrases that build rapport and show empathy [84] since they tend to be technical thinkers with limited soft skills. While these principles may apply to most, if not all customers, interacting with IPV survivors requires extra sensitivity and care, as we discuss below.

**Interacting with IPV survivors.** Training materials for IPV professionals note the impacts of violence on IPV survivors, such as post-traumatic stress disorder and substance abuse, as well as the lengthy and challenging recovery process [4, 59]. Some materials further emphasize *empowerment* — supporting survivors in finding their inner strength [15, 41], and *trauma-informed responses* — understanding the persistent effects of trauma and providing a safe space [58,59]. Others discuss secondary trauma on IPV professionals and respective coping strategies, acknowledging that bearing witness to abuse is emotionally taxing [59,68].

However, most training for IPV professionals does not cover tech-enabled abuse [27]. IPV professionals currently do not have best practices for how to discover, assess, and mitigate tech issues [27]. Meanwhile, support agents at computer security companies provide complementary strength in delivering tech-related assistance, but they may not be sensitive to the nuances in IPV. By synthesizing perspectives from IPV professionals and support practitioners, our work identifies how computer security customer support could help IPV survivors and how this help should be provided.

## 3 Preliminary Analysis of Support Cases

As a starting point, we sought to discover if IPV survivors experiencing tech-enabled abuse seek assistance from computer security companies' customer support and what those interactions look like. We performed keyword searches on customer support records from a large computer security company and surfaced 53 cases in which the customer clearly identified their attacker as an intimate partner. However, typical reactions from support agents indicated they did not recognize the complexity of IPV beyond tech issues.

### 3.1 Method

The company we worked with provides customer support via phone, interactive chat, and self-service (e.g., FAQs, forums, and tutorials). We analyzed chat records since they are anonymized, searchable, and represent a large portion (40%) of support requests. All cases include customer-provided problem descriptions (255 characters maximum). Some cases also include chat transcripts and agents' notes.

To identify relevant cases, we searched a database of 18,900 customer support cases from January 2017 to May 2019. We used search terms[1] indicative of both abusive relationships and IPV-related attacks drawn from prior work [25, 28, 85]. Our initial search surfaced 1,083 cases. After excluding those irrelevant to our interest, such as users reporting generic malware or false positive warnings, we were left with 273 cases of reported interpersonal attacks. Three researchers jointly coded the customer-provided problem descriptions for these cases to identify the attacker's relationship to the victim (Fleiss' $\kappa$=1.00). In 53 cases, the attacker was clearly identified as an intimate partner (e.g., "my partner" or "my ex-boyfriend"). The researchers also coded other attack-related dimensions such as attack type ($\kappa$=0.75), attack mechanism ($\kappa$=0.59),[2] and intimate partner relationship stage as defined by Matthews et al. [53] ($\kappa$=0.82).

We focused on analyzing the 53 cases that decisively indicated tech-enabled IPV. Specifically, we summarized attack-related details based on the customer's problem description, and thematically analyzed the agent-customer interaction based on chat transcripts (if available). Note that other cases in which the attacker's identity was not specified (e.g., "I'm being stalked") may still be IPV-related. Additionally, our analysis did *not* intend to measure the prevalence of IPV cases within customer support data. Our results might not reflect the actual prevalence given that the search terms might have led to over-representation of spyware and ex-partners, and customers might use non-identifying terms to describe attackers who are intimate partners. Rather, the goal was to know *if* such cases occur and qualitatively understand the scenarios support agents are dealing with.

**Ethical Considerations.** Our study received IRB approval. By agreeing to the company's privacy policy, which is prominently featured when a chat session starts, customers consented to chat recordings and messages as examples of diagnostic information being shared with third parties. A company employee reviewed all chat records to verify anonymity and removed references to unique circumstances before providing them to the research team.

### 3.2 Results

**Diverse attack types.** Among the 53 cases, the most common attack types were spying or surveillance of the survivor (23), account or device compromise such as changing the account password to lock the survivor out (17), and interference with account or device usage (12). Less frequently mentioned attacks were harassment (5), spoofing (2), financial fraud (2), phishing (2), and content modification on the survivor's account or device (2). Installing spyware or other malicious apps on the survivor's device was the primary attack mechanism (23), though account compromise based on knowledge of credentials (10) and physical ownership-based attacks (6) also occurred. These attack types and mechanisms generally align with Freed et al.'s taxonomy [28].

**Attacks' repercussions on survivors.** In 49 of the 53 cases, the survivor reported being in the process of separation or had separated from their abuser. Though the survivor's risks might appear lower for attacks after separation, feelings of anxiety and concern were common, with references to violence, ruined lives, and even contemplation of suicide.

In 13 cases, the survivor mentioned multiple types of attack at play, e.g., *"my husband's hobby is to hack my home network and...track my email, calls, and whereabouts."* The attacks caused apparent emotional distress to the survivor, e.g., *"I know that my ex-boyfriend is stalking me through my phone...He has ruined my life."* Another survivor wrote: *"I found out my soon-to-be ex-wife hired a professional hacker to mess me and my folk's computers and phones up...just had a heart attack from the stress."* In six cases, the survivor described that their abuser *"worked at a top IT firm," "can remote access most computers,"* or in other terms that indicate the abuser's tech-savviness. Even though most attacks in IPV

[1] Search terms used: blocked him, bullied, bully, creepy, domestic abus, ex boyfriend, ex girlfriend, ex husband, ex wife, ex-boyfriend, ex-girlfriend, ex-husband, ex-wife, fake sms, fake text, hack my face, hack my what, privacy risk, reading my, reads my, restraining order, seeing my, sees my, spy, spying, stalk, surveil, track, violen.

[2] We did not pursue high inter-rater reliability for this dimension since multiple attack mechanisms were frequently at play.

**Scenario A**

**C:** My ex-husband hacked my phone. He keeps getting my account passwords. I have changed phones so many times and got a restraining order, but he still managed to do this. Please help.

**S:** Thank you for contacting us. I'm happy to help resolve the issue. I would recommend installing [product], which should prevent malware from being installed if you get a new phone.

**C:** I have already spent a lot of money trying to fix this problem and talked to my phone provider. No one has been able to fix it. I can't spend more time and effort on this. Please help, this problem has almost driven me to commit suicide.

**S:** Please do not worry about these devices if you have [product] installed. We will do everything we can to help you further.

**Scenario B**

**C:** My husband is violent and keeps hacking my email and watching everything I do online. Could you help me get him off my network?

**S:** I'm sorry to hear what you are going through. How do you think he is watching your activity?

**C:** He doesn't live with me anymore, but he broke into my apartment last month and I think he hacked my router. I am afraid he can see everything I am doing.

**Scenario C**

**C:** My ex used to share my computer and installed some programs, but I think she installed spyware. I think she is remotely accessing my computer. Can you help?

**S:** Thank you for contacting [company name], I will be happy to assist you. Let's set up a remote connection so I can scan your device for malware. Please visit this link: <link>.

**C:** I can't open it. My computer just restarted. I think she is monitoring this chat and trying to stop me from getting help.

Figure 1: Portions of three representative customer support chats from our dataset ("C" is customer, "S" support agent).

are technologically unsophisticated [28], survivors in these cases expressed being scared and helpless especially when their own computing skills were limited.

**Support agents focused on technical issues.** Our thematic analysis of chat transcripts revealed that support agents were not well prepared for these tech-enabled IPV cases. Figure 1 shows three representative agent-customer interactions. A typical agent reaction was to scan the survivor's device for malicious apps and launch a remote assistance session to investigate further if needed. Agents might also receive out-of-scope requests, as one survivor asked *"I am blocking my wife's/future ex-wife's messages. Is there any way I can have these sent to my email for presentation to my attorney?"* In these cases, the agent would refer the survivor to more experienced experts on the team, device manufacturers, or operating system vendors. For survivors who described traumatic attacks, agents generally expressed confidence in resolving the technical issue but rarely used empathetic language. When survivors suspected hacking or spyware, agents typically reassured that the company's security product would protect them well. Such claims might not be valid, as there were cases in which the survivor expressed skepticism or mentioned having contacted customer support multiple times.

## 4 Focus Groups with IPV Professionals

Our analysis of customer support cases indicates that agents receive help requests from IPV survivors but may not be sufficiently prepared to handle them. To explore how to improve customer support to better serve survivors' needs, we sought input from IPV professionals who have extensive training and experience working with survivors. We conducted five focus groups with 17 IPV professionals between November 2019 and February 2020. We chose focus groups over 1:1 interviews so that participants could listen to each other and collectively discuss ideas. Our study was IRB-approved.

### 4.1 Method

**Recruitment.** Our 17 participants came from five organizations that provide free and confidential civil, legal, counseling, and support services for IPV survivors in two US cities. We explained our study to each organization's director, who then advertised our study to their staff and assisted with recruitment and scheduling. Most participants identified as women and worked as directors/managers or attorneys/paralegals, with diverse years of experience in this field (see Table 1). Participants from G4 primarily served human trafficking survivors, but noted that many of their clients experienced sex trafficking by intimate partners.

**Study protocol.** We conducted in-person focus groups at participants' organizations. Sessions lasted one hour on average and were audio-recorded with participants' consent. We did not compensate participants as the organization directors did not deem it necessary. We prepared a list of prompts to guide the discussion (see Appendix A) and encouraged participants to comment or ask questions at any time. We also used prompts such as "Does anyone else want to chime in?" or "Are there other points of view?" to elicit diverse perspectives and encourage participants to respond to one another.

We started by asking about participants' experience working with IPV survivors, especially regarding tech-enabled abuse. Next, we presented the three scenarios in Figure 1, which represented common attack types in Section 3 and reflected explicit threats from an intimate partner. After participants read the scenarios, we asked them to share their perspectives and recommendations for support agents' role in providing advice, making referrals, and more. We also probed participants to consider adversarial situations in which the abuser might monitor the chat or impersonate the survivor.

**Qualitative data analysis.** We used inductive coding [65] to analyze focus group transcripts. Two researchers independently reviewed and coded the first three transcripts before discussing discrepancies. After agreeing on a consistent codebook, they applied it independently to the remaining tran-

| Group | ID | Gender | Role | Exp. Years |
|---|---|---|---|---|
| G1 | P1 | Man | researcher | 11-15 |
| G1 | P2 | Woman | counselor | 15+ |
| G1 | P3 | Woman | administration | 15+ |
| G2 | P4 | Woman | director/manager | 6-10 |
| G2 | P5 | Woman | attorney/paralegal | 1-5 |
| G3 | P6 | Woman | director/manager | 15+ |
| G3 | P7 | Man | director/manager | 11-15 |
| G3 | P8 | Woman | director/manager | 15+ |
| G3 | P9 | Man | director/manager | 6-10 |
| G3 | P10 | Woman | director/manager | 11-15 |
| G4 | P11 | Woman | attorney/paralegal | 6-10 |
| G4 | P12 | Woman | attorney/paralegal | 1-5 |
| G4 | P13 | Woman | attorney/paralegal | 6-10 |
| G5 | P14 | Woman | counselor | 1-5 |
| G5 | P15 | Woman | administration | 1-5 |
| G5 | P16 | Woman | attorney/paralegal | 1-5 |
| G5 | P17 | Woman | case manager | 1-5 |

Table 1: Demographics and job roles of IPV professionals.

scripts and added new codes that emerged. They then jointly reviewed all coded transcripts, reconciled disagreements, and clustered codes into themes. Our final codebook (see Appendix C.1) has 60 codes, covering topics such as advice to customer support, challenges of customer support, and adversarial scenarios that may involve the abuser. We do not report inter-rater reliability since all data was double-coded and disagreements were reconciled [54].

Next, we discuss IPV professionals' suggestions for how computer security customer support should handle tech-enabled IPV cases in three parts: interactions with survivors (Section 4.2), responsibilities of customer support (Section 4.3), and external referrals (Section 4.4).

While we mention how many groups a topic came up in, we do not include frequencies of themes following recommended practices of reporting focus group data [42]. Frequency cannot reliably indicate importance — some people may comment multiple times on one issue whereas others may not comment at all [42]. Our findings are also qualitative in nature and based on a small sample size. Frequencies could be misleading when taken out of context and projected onto a population [42].

## 4.2 Suggestions for Interacting with Survivors

IPV professionals provided three key recommendations for interacting with customers who might be IPV survivors: using trauma-informed language, asking follow-up questions without judging, and avoiding overpromising.

**Use trauma-informed language.** IPV professionals reacted strongly to the language support agents used to respond to survivors' concerns. Four groups said that Scenario A included dismissive language that might mislead or re-traumatize the survivor. Professionals took issue with the phrase "please do not worry about these devices if you have [product] installed," noting that it is highly inappropriate to focus on the security software's functionality right after the survivor mentioned a restraining order on their abuser and suicidal thoughts. An attorney discussed how the agent's language might arise from the goal of making customers happy in their regular work:

> *"I understand that the role of customer support is to make their customer feel better. But this is just a space where . . . they have a limited capacity to make [the survivor] feel better . . . I think the goal should be to hear and be honest about the limitations of what [product] can or cannot do in those moments."* (P11, attorney)

All groups highlighted the importance of trauma-informed language, a common element in their own training and practices [58, 59, 66] and in other fields serving trauma survivors [1, 52, 62]. Being trauma-informed means accounting for the pervasive nature of trauma and avoiding unintentional re-traumatization through careful language and interactions [23]. A counselor explained how to provide trauma-informed responses in customer support:

> *"Acknowledge that 'this is scary' and that 'it sounds like you're having a really hard time.' Even just the smallest little pieces of empathetic language so [the survivor] knows that [the agent] is actually hearing them . . . and expressing concern for them."* (P2, counselor)

Professionals provided suggestions for training support agents to use trauma-informed language, such as using the Forensic Experiential Trauma Interview (FETI) [12], which is aimed at law enforcement but makes analogies for people who do not typically work with survivors. Another suggestion was incorporating trauma-informed responses into scripts, so agents do not need to figure out what to say on the fly. Nonetheless, scripts alone were considered insufficient: part of the training should be educating agents about the complexities of IPV and why trauma-informed responses are needed.

One group highlighted the need to address support agents' own trauma. Due to the prevalence of IPV [8, 78, 79], some agents may be survivors themselves. Agents may also feel distressed and helpless hearing survivors' experiences:

> *"Some of these calls will be harmful to the people who receive them. They'll be really traumatized by these experiences . . . Any company that's recognizing their frontline employees are experiencing these phone calls needs to think about how to support employees through secondary trauma issues and process it."* (P13, legal advocate)

**Ask follow-up questions without judgment.** Four groups suggested that agents could ask follow-up questions to surface additional risks that should be considered when giving advice and ensure that the customer is safe to receive and act on advice. The question, "How do you think he is watching your activity?" in Scenario B was identified as a good example: it is open-ended, non-judgmental, and might help the agent better diagnose the case by encouraging the customer to speculate about the source of the problem.

Professionals also provided their own examples of appropriate follow-up questions, e.g., asking about the customer's immediate concern in the form of "What are you most concerned about?" or "What is your goal of calling me today?" Professionals explained that such questions do not assume the survivor's needs and might help identify other risks that warrant attention, such as those related to immigration status, health, or economic situation. Another follow-up question could be, "What have you already tried?" to facilitate the troubleshooting process and make the conversation more productive, since the survivor likely tried to address the problem before reaching out for help.

Professionals further discussed the need to account for the possibility that the abuser might be physically or remotely accessing the survivor's devices and accounts. Four groups recommended a safety check-in with the customer by asking, "Do you think you're on a secure line?" or, "Are you safe now?" If the response is no or unsure, the agent should offer to call back or initiate a chat from a different device, such as a friend's phone. Three groups also recommended verifying the customer's identity in case the abuser is impersonating the survivor to gain access to the security software or other accounts. The agent could verify the customer's email, phone number, or account history (e.g., "I see in our records someone just called about this account. Is that you?").

Nevertheless, professionals acknowledged that it is challenging to handle situations in which the abuser is present: identity verification takes practice and can still go wrong; giving advice such as switching to a different phone might tip off the abuser. Yet, professionals noted that the risk does not undermine the importance of support agents providing necessary help and information. As a researcher explained:

> *"[The survivor] had to disclose the problem to begin with, so [the abuser] has already [been] tipped off. But . . . that's why we need to connect [the survivor] to a safety clinic. It's really tricky when the phone is the only way to communicate."* (P1, researcher)

**Avoid overpromising.** All groups took issue with the phrase, "I'm happy to help resolve the issue" in Scenario A, saying that "resolve" is an overpromise because one chat session is unlikely to solve the physical and digital complexities survivors face in IPV [27,28,53]. From their perspectives, agents might promise to solve problems instinctively or to comply with company policy. Yet many IPV survivors face persistent attacks from their abusers and are likely experiencing effects of trauma, meaning that such promises could be misleading and frustrating to them. Professionals noted that a better response would be to be honest about the security software's limitations while still providing support, such as, "I will help you as much as I can in this call today, and whatever we don't take care of, we might have to keep working on it." Doing so does not necessarily contradict the agent's responsibility to help customers. As a legal advocate said:

> *"[The agent] can still support the survivor while giving them a response they don't want . . . But do it in a way that lets [the survivor] know they are there, they understand, they are validating their experience . . . They can still give [the survivor] bad news without completely turning them down."* (P16, legal advocate)

## 4.3 Responsibilities of Customer Support

Customer support's typical role is to provide technical assistance related to the company's products and services and engage with customers [7]. Professionals stressed that while agents should only advise on topics within their expertise and refer the customer elsewhere for issues beyond, agents could do more than troubleshooting technical problems or recommending the company's products. For instance, agents could discuss the potential consequences of advice they give or share basic technology safety tips.

**Avoid making advice too product-oriented.** In Scenario A, the agent recommended installing one of the company's software products. Professionals commented that this behavior is understandable, given that the agent represents the company and that the product might be helpful. Nevertheless, the line might read too product-oriented and convey the impression that the agent was following a script and making a sales pitch without actively listening. To make a product recommendation more helpful, a counselor suggested explaining how and why the software is going to help in the survivor's situation:

> *"[The survivor] didn't call for that product. She called with a problem. [The agent] never explained how their product was going to solve the problem . . . so please give more explanation about that."* (P2, counselor)

**Discuss consequences of given advice.** While professionals agreed that support agents could provide IPV survivors with vital assistance, they emphasized the caution required in providing such assistance. One suggestion was explaining potential negative consequences that might result from the advice to prompt the survivor to consider safety issues. A manager gave an example:

> *"Ask [the survivor]: if this app were to be uninstalled, how would it affect you? . . . Do you use it often? Do you rely on it? Does the [abuser] have access to it? Will they notice if it's uninstalled?"* (P9, manager)

However, other professionals mentioned a potential issue with discussing negative consequences — it might trigger additional questions from the survivor that catch the agent off guard, which points to the importance of external referrals:

> *"I feel it's like a slippery slope because [the agents] are not domestic violence advocates. And so [the survivor] is going to just be like, 'What do you mean? What do you think will happen?' And they're never going to be able to answer those questions."* (P1, researcher)

**Share resources for tech safety.** Three groups suggested sharing resources that might improve the survivor's digital security and privacy, such as adjusting privacy settings on social media and using strong passwords. Prior work with IPV survivors [26] also indicates that survivors have many general tech safety questions and desire credible information on this topic, validating the need for sharing tech safety resources. One group noted that in addition to sharing existing resources, such as the NNEDV's Safety Net project [76], computer security companies could utilize their expertise to provide self-created content on tech safety. Such content could appear on the company website's FAQ or "Contact" page to put such resources into a survivor's pathway of seeking help.[3] Participants suggested tech safety resources be written in plain language and provided with non-technical support resources (e.g., information about domestic violence shelters) to ensure relevant resources are available in one place.

**Have a specialized team.** Three groups suggested a specialized team within the company's customer support division for handling IPV cases transferred from frontline agents. A specialized team resolves the dilemma for frontline agents who are often pressured or incentivized to complete cases quickly [63], whereas dealing with complex issues like tech-enabled IPV requires extensive effort and patience. It could also reduce the company's workload in coordinating training, as training a small group of specialists would be easier than training all frontline agents. One group further noted that the company could track the number of potential IPV cases frontline agents receive to understand the issue's prevalence and decide whether investing in a specialized team is warranted.

Given the possibility that a survivor might face imminent danger, professionals emphasized that frontline agents should always conduct a safety check-in (e.g., "Do you think you can stay on the line with us?") to determine whether the survivor could tolerate a transfer to the specialized team. Additionally, many survivors might have experienced prior failures in obtaining assistance and could easily get frustrated when being transferred. A counselor gave an example of appropriate language taking this into account:

> *"We, as a company, remain interested and committed to trying to help you and talk to you . . . But if you can hold on a minute, I'm going to get you connected with a colleague who knows our product but can [also] talk to you about some of these [safety] issues."* (P2, counselor)

Without the pressure of completing cases in a limited time, professionals envisioned that these specialist agents could even build long-term relationships with survivors, such as following up with them if the problem does not get fixed in the initial chat session. Importantly, four groups cautioned that support agents should never provide advice beyond their expertise and training. Examples of out-of-scope advice included comprehensive IPV-related counseling, safety planning (e.g., maintaining physical safety in leaving an abuser), and legal advice. While professionals identified a handful of follow-up questions to ask or advice to give, they noted that the extent to which agents can help customers think through potential consequences depends on the individual's situation and needs. If the survivor needs support the agent cannot provide, the agent should refer them to external professionals with expertise in the social, legal, or health aspects of IPV.

## 4.4 Suggestions for External Referrals

In addition to technological challenges, many IPV survivors are concurrently dealing with medical, legal, financial, and other complex problems [27]. With this in mind, professionals discussed the need to refer survivors to external support, including IPV advocates, legal experts, and law enforcement. We now discuss professionals' suggestions on *where*, *when*, and *how* to refer survivors to external organizations.

**Where to refer.** All groups stressed the need to refer survivors to relevant hotlines (e.g., the National Domestic Violence Hotline, Safe Horizon, and Crisis Text Line) and organizations that provide resources for survivors (e.g., NNEDV). Four groups also suggested referrals to 911 or the National Suicide Prevention Lifeline if there are cues of physical danger or suicide contemplation. Two groups mentioned that survivors might also benefit from referrals to legal resources (e.g., WomensLaw.org) or sex trafficking resources (e.g., the National Human Trafficking Hotline).

One challenge in making referrals is that the resources available differ substantially across local, state, national, and global boundaries. In the US, there is the National Domestic Violence Hotline, but each state also has its own hotline [81]. The referrals get more complicated for global companies. However, a legal advocate argued that figuring out the exact resource for referrals is not necessary as long as any referral is given, as staff at hotlines and organizations are sufficiently trained to refer onward if they are not in a position to help:

> *"Most of these places that you call can handle any of these intakes and they'll figure out the way . . . If you get the company committed to giving out a suicide hotline and a collection of these numbers, honestly the distinctions don't matter."* (P13, legal advocate)

[3] Some security companies are already doing this (e.g., [37,51]), although most content does not specifically address IPV or tech-enabled abuse.

**When to refer.** To determine when an external referral is needed, all groups suggested monitoring for "red flags" in the conversation. Indications of adverse behaviors such as spying, stalking, and violence from an intimate partner generally point to the need for IPV-related resources. "This problem has almost driven me to commit suicide" in Scenario A or other indications of threatened physical safety are clear red flags that call for 911 and suicide prevention resources.

Three groups suggested that agents be trained to understand and identify common types of tech abuse. One resource that could be part of such training is the NNEDV's Power and Control Wheel on Technology and Abuse [75]. For situations without clear indications of IPV (e.g., the customer mentions abusive behaviors but does not mention an intimate partner), professionals believed the agent should still share relevant resources not limited to IPV. An attorney gave an example:

> *"If it's a stranger, there would have to be some concerning conduct ... So if [a customer is] calling, maybe it's because [they] are getting creepy spoofed messages from an account [they] don't recognize. Well that's already raising flags, right?"* (P5, attorney)

In Scenario C, in which the customer believed their ex was monitoring the chat to prevent them from getting help, one group pointed out this was an example of controlling behavior that still warrants attention, as IPV can occur via coercive control without physical violence [14, 16, 29]. Professionals across all groups advocated for making referrals without worrying about verifying whether the customer is experiencing IPV: a referral is better than no referral, because not providing resources to someone in need can do more harm than providing resources to someone who does not need them:

> *"Let's say [the customer] is actually safe ... They Google the number, they see it's ... the domestic violence helpline. They're going to be, 'whatever, I'm not calling that' ... But for the person who really has the need, if they want it, they will follow up on that phone call.*" (P12, paralegal)

**How to refer.** Four groups mentioned an important principle in making referrals was to respect the survivor's agency in decision making. The idea of empowerment — that survivors should be able to decide if and how they want to get help — is common in IPV professionals' training [57, 59]. As an example, an administrative assistant explained that agents should always ask survivors whether and how they would like to be transferred to external resources:

> *"Maybe this survivor is not in a private space to have that conversation ... Maybe transferring them directly to a domestic violence agency [is] too overwhelming at that moment and not what they are looking for ... Give them resources to explore it on their own."* (P15, admin. asst.)

Three groups discussed potential harms resulting from labeling the customer as an IPV survivor. Here, the harm does not come from the action of providing IPV-related resources, but rather from repeated mentioning of words like abuse, domestic violence, or victim. Customers who are not survivors might find it offensive, and customers who are survivors might not be ready to be identified as such. Instead, agents should use the same language that the customer uses, e.g., if the customer describes abusive behavior from an ex-partner, the agent should also use "ex-partner" in referring to the abuser. As a counselor described:

> *"If [my clients] say something is going on, I am not going to say 'you are a survivor of domestic violence' ... You don't want them to think that the person has assumed ... You want to give them the opportunity to call it in whatever ways they want."* (P14, counselor)

## 5 Focus Groups with Support Practitioners

IPV professionals provided many suggestions for how customer support could provide help for IPV survivors. To assess the practicality of these suggestions, we conducted four focus groups with 11 customer support practitioners between April and June 2020. We sought to learn how attuned support practitioners are to tech-enabled IPV and their opinions on these suggestions, including any potential implementation challenges. We continued the focus group format, considering that IPV could be a new and sensitive topic to support practitioners, and that a group setting may make participants comfortable sharing their thoughts upon hearing others' opinions or experiences [27, 57]. This study also received IRB approval.

### 5.1 Method

**Recruitment.** Our participants came from four large security companies affiliated with the Coalition Against Stalkerware [71]. All four companies offer consumer- and business-facing security software and services to millions of customers. Each had customer support divisions to answer product-related questions and concerns. Among our participants (see Table 2), all but two identified as men. The majority had been in the industry for 5+ years. Half of our participants were directors or managers; the rest held diverse roles. While researcher and content writer might sound irrelevant to customer support, both participants mentioned experiences with tech-enabled abuse cases in initial email exchanges and contributed relevant insights in the focus groups.

**Study protocol.** We conducted focus groups remotely over video chat since participants were geographically dispersed. We synthesized our results from Section 4 into a presentation in five parts to guide the discussion (see Appendix B).

| Group | ID | Gender | Role | Years |
|---|---|---|---|---|
| G1 | S1 | Man | training consultant | 11-15 |
| G1 | S2 | Man | engineering & support liaison | 6-10 |
| G2 | S3 | Man | director/manager | 6-10 |
| G2 | S4 | Man | director/manager | 11-15 |
| G2 | S5 | Man | director/manager | 11-15 |
| G2 | S6 | Man | director/manager | 11-15 |
| G3 | S7 | Woman | director/manager | 11-15 |
| G3 | S8 | Man | content writer | 6-10 |
| G3 | S9 | Woman | support specialist | 11-15 |
| G4 | S10 | Man | director/manager | 1-5 |
| G4 | S11 | Man | researcher | 1-5 |

Table 2: Demographics and job roles of participating customer support practitioners.

In Part 1, we explored participants' backgrounds, their company's customer support organizational structures, and metrics for measuring success. We also asked if participants had encountered tech-enabled IPV cases in their roles (either personally or through a team member) and any company initiatives to support IPV survivors. In Parts 2–4, we presented summaries of IPV professionals' suggestions: how to interact with survivors (Section 4.2), the responsibilities of support agents (Section 4.3), and how to refer survivors (Section 4.4). In Part 5, we elicited feedback on IPV professionals' suggestions for training components (e.g., common types of tech-enabled abuse, trauma-informed responses, and secondary trauma). Each part contained specific examples and quotes from our focus groups with IPV professionals. We invited participants to freely share their reactions and thoughts on the value, cost, feasibility, and challenges of putting the suggestions into practice. Similar to our method in Section 4.1, we used probes to elicit different opinions and encouraged participants to engage with each others' ideas.

**Qualitative data analysis.** We used inductive coding [65] to analyze focus group transcripts. Our coding process was similar to Section 4.1: two researchers independently coded two transcripts, compared differences, created a consistent codebook, applied the codebook to the remaining transcripts separately, and reviewed all coded transcripts together. Our final codebook (see Appendix C.2) has 49 codes and covered topics such as customer support's existing practices, reactions to IPV professionals' suggestions, challenges of implementation, and new ideas for supporting IPV survivors.

## 5.2 Well-Received Suggestions

Practitioners agreed on the importance of assisting IPV survivors and training frontline agents for this purpose. Practitioners also endorsed the idea of providing and sharing tech safety resources, which they had been doing to some extent.

**Existing practices to support survivors.** Practitioners in all groups reported having received tech-enabled IPV cases in their roles, confirming the need for customer support to assist survivors. Although no company had a protocol to respond to IPV cases specifically, each company had a specialized team for handling complex cases transferred from frontline agents, such as malware-related issues that demand more time and expertise. S9,[4] a customer support specialist, mentioned sharing a license key of their product's premium version with customers experiencing IPV. Agents also ask each other for advice when encountering unfamiliar cases:

> *"Even though we don't have formal training or content around such issues ... out of experience, we do share some information on how we can handle such customers ... Higher tier agents actually talk to [frontline agents] and guide them appropriately."* (S1, training consultant)

**Train agents on tech-enabled IPV.** Three groups acknowledged the importance of training agents for cases of tech-enabled IPV, recognizing that these cases were happening and that agents did not have an established protocol to follow. A director noted that even if a specialized team exists, frontline agents still need to receive training that covers the complexity of IPV and the role of technology in facilitating abuse:

> *"We [can have] a specialized team which ... knows exactly about next steps. But the first contact is regular support agents, who have no dedicated training on this, and therefore there must be at least the awareness that these kind of privacy issues, stalkerware ... could be on the device."* (S10, director)

Another director liked the idea of embedding trauma-informed responses in training, noting that such responses would benefit all customers, not just IPV survivors:

> *"We do a lot of this already in terms of what we call the empathy phrases or scripting. I think this is something that could be done regardless of whether or not I'm interacting with someone that is dealing with trauma or IPV. This should be used across the board."* (S6, director)

Practitioners contributed ideas on training. S1, who created training content for their company's support agents, suggested basing materials on stories or scenarios so that agents could quickly draw connections to cases they encounter and identify potential solutions. S10, a director, emphasized that training should be offered regularly to keep up with the evolving spyware landscape.

**Address agents' secondary trauma.** Two groups reflected on the necessity of providing mental health support to agents

[4] We use "S[number]" as identifiers for support practitioners to differentiate them from IPV professionals.

who interact with IPV survivors and witness the tech-enabled abuse they are experiencing. The notion that support agents themselves might be survivors provoked reflection:

> *"Didn't even consider that. It's funny that considering the stats . . . I got a hundred [agents] on the floor, odds are some of them have been affected by this."* (S6, director)

S8, who maintained their company's blog on digital rights and anti-stalkerware initiatives, noted the psychological toll in dealing with IPV cases especially for newcomers:

> *"These stories add up. I think they take a toll on us, particularly for people who aren't aware of them. For people who [first] learned about how prevalent this problem really is, it can be a bit of a shaky, shattering moment for them."* (S8, content writer)

**Share tech safety resources.** In line with IPV professionals' suggestions, practitioners from all groups reported that their company was already providing customers with general tech safety advice under certain circumstances. Examples of such advice included performing a factory reset when getting a new phone and using a password manager if the customer reports account hijacking.

Practitioners further expressed interest in providing curated content to educate customers about security and privacy. Given that all companies already had a website with basic online safety advice, practitioners viewed adding articles about IPV and tech-enabled abuse as a low-hanging fruit of critical importance. A director stressed that tech safety alone might be insufficient for survivors and should come with external resources, similar to the IPV professionals' suggestions:

> *"This could be quite easily done . . . setting up this knowledge base article, help center . . . and giving the guidance of 'These could be potential steps to take in consideration of safety planning. Get in contact with . . . organizations that can support you.' "* (S10, director)

**Make referrals.** Practitioners considered referrals to external organizations achievable. Three groups said they already did this to some extent, e.g., by directing victims of online scams to a governmental fraud investigation team. A director described a case of referring a customer to law enforcement:

> *"We've gotten requests in the past where people have said, 'Hey, I think my husband is hacking my computer. Can you find their IP address and do all this stuff for us?' I'm like, 'Well, we can't do that for you. If you suspect that something's going on, first let's make sure that the [product] is installed and running properly to protect any type of intrusions . . . If you still have concerns, then contact the local police and report.' "* (S6, director)

Practitioners commented that expanding the scope of their current list of external referrals would improve the process without negatively impacting agents' capacity. However, practitioners also noted that referred resources should be up-to-date and relevant, which requires maintenance efforts. Moreover, sharing geographically applicable resources could be challenging for companies that operate on a global scale.

Regarding the idea of creating an internal specialized team to handle tech-enabled IPV cases, three groups mentioned budget and capacity barriers, particularly in the face of financial constraints due to the COVID-19 pandemic. Two groups further suggested tracking the number of relevant cases to inform this decision, echoing IPV professionals' suggestions. As a director told us:

> *"I think our founder would have a genuine interest but I think we'd also need to balance that with business needs . . . We need to get a better sense of how many calls we have coming in that . . . go more towards violence and partners taking retaliatory behavior."* (S3, director)

## 5.3 Implementation Challenges

Practitioners discussed challenges in implementing some of IPV professionals' suggestions. Some practitioners questioned whether customer support, as experts on products and technical issues, should intervene in IPV cases. Others worried that frontline agents have limited capacity to help and might struggle to identify survivors who need help.

**Uncertain role of customer support.** Two groups expressed uncertainty about the role of customer support in addressing tech-enabled IPV. From their perspectives, agents should play the traditional role of customer support — focus on the product and make customers happy. They were hesitant to let agents "take sides" in IPV situations. A director said:

> *"The agent's role is to focus on the product. Because we don't know what's going on in the customer's life . . . There's the rights of the person that's calling us as well as the rights of the individual being accused. It's best not to take sides and just stay neutral."* (S6, director)

Other practitioners expressed confidence in their products, viewing them as the ultimate solution for most customers including survivors. A training consultant considered increasing customers' confidence in the product as the end-goal:

> *"[Customers] need to get confidence in [the agent] they talk to, that here, this person knows what technology is . . . whatever workaround that person is providing, if they follow that, then they don't have to worry any further about . . . being [the] victim of technological abuse."* (S1, training consultant)

While a commitment to providing customers with high-quality technical solutions is essential, the confidence in security software's ability to fully protect survivors contradicts the caution requested by IPV professionals, who viewed overpromising as frustrating and dangerous for survivors. Nonetheless, not all practitioners shared this overconfidence. A researcher agreed that agents should not overpromise and drew connections to a case in which the attacker was configuring the victim's Google accounts for location tracking:

> *"In this case, technically our detection could not help, because this was actually done through the official Google apps . . . We are aware of what stuff can go on, and we are careful not to overpromise . . . pushing [our] product or anything."* (S11, researcher)

S10, who came from the same company as S11, similarly acknowledged their product's limitations and the importance of safety planning in removing stalkerware from the survivor's device. They further illustrated how agents could explain the situation to a survivor:

> *"We cannot support you in the full steps but we know organizations you can [get] in contact with . . . If you discuss the safety planning [with] them . . . then you can come back and discuss with us how we [can] remove the app from your device."* (S10, director)

**Identifying potential survivors is challenging.** IPV professionals argued that customer support should not be conservative in making referrals. By contrast, support practitioners tended to focus more on accurately identifying survivors who might need referrals and saw challenges to this end. In response to IPV professionals' suggestion to familiarize agents with common types of tech abuse, a director said this would not be effective without self-disclosure from the survivor:

> *"That's a good idea but in practice would be difficult . . . I think it's really going to be the customers coming forward and saying that this is happening. That would trigger stuff on our end to handle it differently."* (S6, director)

Another director noted that most customers do not have extensive technical knowledge and struggle to describe issues accurately, making it challenging to diagnose the problem:

> *"The victims may be aware that something is wrong on [their] phone, but cannot really describe what the issue is about . . . or maybe [they] describe it [on] a high level."* (S10, director)

As one solution, a practitioner proposed using probing questions to confirm the customer's "survivor" identity. However, we caution that such questions, especially those on the history of abuse, might unintentionally re-traumatize the customer, and differ from IPV professionals' suggestion to consider additional risks and attack vectors rather than to verify the IPV situation:

> *"We do some verification for customer contacts . . . where we collect basic information like name, email, address . . . But I don't know, it's not foolproof to see if they were actually victims of abuse. Or by giving them some open questions like, how were they victimized? Having them quote some examples that can give us a sense?"* (S2, engineering & support liaison)

**Complexities of tech-enabled IPV.** Practitioners discussed the socio-technical challenges in IPV and the resulting problems for support agents. All groups mentioned the dual-use nature of many apps used by abusers [10] as a challenge. A director described training agents to watch out for dual-use apps:

> *"Sometimes [agents] have to make some additional changes to . . . our software to categorize those types of gray applications as malicious so that it can be removed. Our agents are trained on that so that's probably one of the first things they would do."* (S6, director)

Another director considered the possibility that the abuser might be monitoring the conversation, and simply removing the stalkerware might put the survivor at further risk:

> *"Just to say, 'Hey, your device is infected' and remove the stalkerware typically means a risk for the victim . . . We don't see [an] ideal way of communication if we identify stalkerware on a device, because the victim most likely gets observed on all channels . . . If we shot them an email to their Google account . . . the attacker can see this communication. Just removing without notification, a victim could also be at risk because the attacker assumes that the victim is aware."* (S10, director)

**Frontline agents have limited capacity.** On top of challenges in identifying and addressing tech-enabled IPV, two groups pointed out that support agents already work hard and have little time or capacity to take on new and complex tasks. S7, a manager, described frontline agents as *"the Cinderella of companies"* with the lowest pay but the expectation of doing a perfect job. In response to IPV professionals' suggestion that agents mention possible consequences of given advice, S8 was concerned that there may be too many consequences for frontline agents to foresee, pointing to the importance of external referrals for safety planning:

> *"My answer is trust the National Domestic Violence Hotline. Call them from a safe device. But that's it. There really isn't a one-size-fits-all answer on this. [Safety planning] is something that takes more than a couple of minutes . . . I could not see that happening in under an hour."* (S8, content writer)

## 6 Discussion

Our findings show that support agents already encounter cases of tech-enabled IPV. There are many ways customer support could help survivors and challenges to them playing this role. We now note limitations of our work, reconcile perspectives between the two sets of focus groups, and discuss areas computer security companies can explore to improve their customer support for IPV survivors.

**Limitations.** Our research has several limitations. Our sample sizes were on the lower end for focus group studies [55]. Both groups were hard-to-recruit populations due to their specialities and limited time; customer support practitioners' participation further required their companies' approval. Nevertheless, we believed our recruitment was sufficient, as data saturation was reached before we stopped data collection.

Our findings have limitations in terms of generalizability. While the participating companies are leaders in the consumer security market globally, the IPV organizations are all based in US metropolitan areas. We recruited support practitioners from companies in the Coalition Against Stalkerware [71] which are already committed to fighting tech-enabled abuse; other companies who have not expressed such commitment might be less amenable to adopt our recommendations. Our focus on computer security companies is warranted, but other customer-facing domains (e.g., banking and insurance) also assist IPV survivors in managing consequences of abuse and could offer targeted assistance. Future research could examine to what extent our recommendations apply to these domains.

**Security software is not a silver bullet.** Existing anti-virus and anti-spyware tools have limitations in detecting dual-use apps used for intimate partner surveillance [10]. Even with improved detection algorithms [64], security software cannot fully protect IPV survivors as they face complex social and legal challenges [27,39]. IPV professionals unanimously agreed that security software is not a silver bullet for addressing tech-enabled IPV, and coordination with other stakeholders in the IPV ecosystem is vital to providing survivors with holistic support. Some customer support practitioners acknowledged their products' limitations and the importance of not over-promising, but others sought to give customers confidence in provided solutions or believed that their software would protect most customers by default. The divergent opinions between practitioners from different companies reflect that a mentality change in dealing with IPV cases must occur at the company level — pursuing perfect technical solutions might be reasonable for general customers, but could be dangerous and misleading for IPV survivors. Agents should communicate the benefits of a technical solution while acknowledging that successfully resolving a tech issue at the moment is unlikely to resolve all of a survivor's problems.

**Provide IPV tech advice with caution & boundaries.** IPV survivors face risks of escalated abuse for even routine privacy-protective measures like turning off location tracking or changing passwords [27,28,40]. As such, for any technical solutions provided, agents should be equipped to recognize the potential repercussions on survivors and recommend alternative solutions that account for an abuser's potential control of the survivor's accounts and devices. As noted by both IPV professionals and support practitioners, for survivors with suspected spyware on their phone, agents should highlight that any activity on the device may be seen by the abuser and ask the survivor to consider how to proceed instead of simply removing the spyware.

Furthermore, IPV survivors who contact computer security customer support likely have a wide range of needs based on their situation. While prior work has identified different phases of IPV [53], our findings suggest that the advice provided by support agents can and should be IPV phase-agnostic: trauma-informed language benefits a survivor before and after separation as trauma persists, and caution around an abuser's potential monitoring or escalated violence is needed in all phases. Customer support agents should not offer advice that requires them to know the details of a survivor's living situation, contact with the abuser, or plans for leaving. Neither should support agents ask about these details, as the questions can be traumatizing and invasive. Instead, support agents should provide options, highlight risks, and rely on the customer to make the safest decision for themselves. Any in-depth safety planning that helps survivors remain safe in escaping and requires knowing the phase of IPV should be handled by IPV professionals via referral. By recognizing their work's boundary and facilitating the connection to external resources, support agents increase the chance that a survivor gets the help they need with precaution.

**Make external referrals for safety planning.** IPV professionals and support practitioners both emphasized the importance of external referrals. All companies we spoke with were already referring customers to certain external resources such as law enforcement, so the infrastructure and general procedure for doing this are in place. An immediate next step is to add domestic violence hotlines, human trafficking hotlines, suicide helplines, and others to the repertoire of referred resources. As support practitioners noted, the provided resources should be up-to-date and geographically relevant. Even though some regional organizations (e.g., the National Domestic Violence Hotline in the US [36] and the Women Against Violence in Europe [21]) maintain lists of state and local domestic violence hotlines and can refer survivors onward, many countries lack a national hotline for domestic violence [60], indicating the need of broad referrals for survivors in these areas. Pointers to external resources could also be embedded under the company's FAQ or other tech support pages, as this approach further increases survivors' access to resources with low chances of triggering the abuser when they only pay attention to the page title or web address.

Regarding the specific processes in making external referrals, support practitioners and IPV professionals noted different challenges. Support practitioners highlighted challenges around *when to refer*: not only recognizing signs that someone might need a referral, but also doing enough vetting to determine that the customer was definitely experiencing abuse. IPV professionals did not consider the latter point necessary or advisable, as it could lead to presumptive labeling or traumatizing questions. Instead, they emphasized that whenever there are red flags indicating a need for further assistance, agents should provide referrals. They were mainly concerned with *how to refer*, and suggested that agents use respectful language in offering referrals, avoid labeling, and give customers enough agency to decide whether they need or want to act on it. For high-stakes situations like IPV, ensuring whoever needs resources can learn about them takes priority, and recommending resources with non-judgmental language does not harm customers who do not need them. By offering referrals, support agents are not "taking sides," but rather serve as crucial bridges to social workers, attorneys, law enforcement, and other IPV experts.

Note that avoiding harmful labeling does not mean agents should be vague in describing the referral resources and associated risks. Survivors should be given a clear picture of the referred organizations to account for potential repercussions from the abuser. For instance, when sharing the number of a helpline, agents can use the same terms used by the survivor to avoid labeling while still being explicit about the audience it serves. Agents should further caution that the number, if called, would be in the call history and might be seen by the abuser; a safer option may be to call from a friend's phone or a public phone. Additionally, agents should not treat all digital abuse victims as IPV survivors by default. Targeted digital attacks also occur to NGO employees [44], politicians [30], journalists [82], and in the context of elder or child abuse [2, 56]; the victims bear similarities to IPV survivors but have distinct vulnerabilities. Ideally, agents are trained to generally recognize such situations, use trauma-informed responses, and make referrals to related resources if needed.

**Train customer support agents.** IPV professionals and support practitioners unanimously agreed that training frontline agents to be better prepared for tech-enabled IPV cases is both feasible and critical for supporting survivors. Support agents are already dealing with these cases. Survivors who contact computer security companies may not be aware of existing IPV-related resources, and some may not even realize they are facing tech-enabled IPV. Therefore, having more potential contact points, including but not limited to support agents who receive training in identifying signs of tech-enabled IPV, is an essential step in raising survivors' awareness and providing them with necessary help. Equipping agents with a basic understanding of IPV and the caution needed for a proper response is also vital to prevent inadvertent harm, such as escalating abuse by removing spyware without further precautions or making misleading promises.

Based on our findings, we identify the following components as potential elements of such training. We have developed respective training materials and shared them with one of our partner companies, who provided positive feedback.

1. *Introduce IPV to customer support agents.* Discuss the prevalence of IPV, including technical (e.g., how technology is misused to facilitate IPV) and non-technical aspects (e.g., the survivor's and abuser's social entanglements and the need for holistic safety planning). Explain why agents should be committed to learning how to support survivors.

2. *Describe common tech-enabled abuse and desired responses.* Present scenarios of how abusers exploit technologies in IPV and model how agents should respond. Define and give examples of trauma-informed language, and explain its importance. Frame the problem as an opportunity to offer help rather than a situation that requires careful vetting or evaluation of the customer's victimhood.

3. *Explain how agents could provide support.* Present methods for assisting survivors, such as asking questions that take into account broader risks beyond the immediate tech issue, sharing tech safety resources, and making referrals.

4. *Identify mental health resources for agents.* Provide resources (e.g., therapeutic sessions and peer support groups) for agents who might be experiencing IPV or suffering secondary trauma from handling such cases.

Ultimately, training should make agents aware of unique risks and nuances in IPV, help them pick up cues that indicate customers experiencing IPV, and teach them how to safely and respectfully share resources. As support practitioners noted, training should be updated and provided periodically to strengthen recall, as frontline agents might not encounter IPV cases frequently enough to practice applying the knowledge. Furthermore, training components like trauma-informed language provide benefits beyond IPV survivors. For example, victims of hacking and identity theft are also dealing with complex tech issues and distress in their lives [9, 43], and would benefit from interacting with agents that use trauma-informed language.

**Track IPV cases to inform decision-making.** Some IPV professionals proposed having an in-house specialized team for IPV cases to reduce the pressure on frontline agents and save effort in training everyone. However, support practitioners responded that justifying the cost of building this specialized team is difficult when the company does not know how frequently their customers would need it. Both sets of focus groups brought up the idea of tracking anonymized data of tech-enabled IPV cases in support agents' daily work. Doing this would provide insights into the frequency and types of attack mechanisms, how agents handle these cases, and the extent to which agents may experience secondary trauma. Such knowledge can guide companies in making business decisions, including a specialized internal team to support survivors and beyond, and identify other opportunities to help IPV survivors and support agents.

**Build partnerships between security companies and IPV advocates.** Tech-enabled IPV is likely to persist, indicating the need for coordinated expert support. Both computer security companies and IPV advocacy groups are vital to the support ecosystem. Our research synthesizes the expert advice from IPV professionals and support practitioners, who each have in-depth knowledge of constraints in their professions. As tech-enabled IPV grows in prevalence and changes its forms, new countermeasures are needed to protect survivors. An enduring partnership between IPV support organizations and computer security companies provides learning pathways for both parties. IPV professionals can receive guidance on recognizing signs of spyware and other abuse-enabling technology in their work. Security professionals can learn about guidelines for interacting with survivors and incorporating them into protocols for customer support and beyond. For example, spyware detection tools would also need to consider that the notification may escalate violence when read by the abuser, and inappropriate language may re-traumatize the survivor.

We further envision coordinated approaches to help survivors via this partnership. Instead of sporadic referrals to domestic violence hotlines, computer security companies and IPV professionals could work together to deploy remote security clinics [80] with digital safety planning for individual survivors. An established partnership could increase IPV professionals' confidence in referring their clients to computer security companies that are committed to knowledgeably and compassionately assisting survivors. Notably, support agents and IPV professionals should reach a consensus about their own responsibilities in such a collaboration — support agents for technical issues and basic tech safety tips; IPV professionals for comprehensive safety planning and non-technical assistance — so that survivors do not end up being referred back and forth between these parties without getting help.

## 7 Conclusion

IPV is a pervasive problem that increasingly manifests in the digital realm. Supporting IPV survivors who are experiencing tech-enabled abuse requires the expertise of multiple stakeholders. We discovered real-world support cases involving IPV at a large computer security company, elicited IPV professionals' opinions on how customer support could assist survivors, and explored the feasibility of implementing their proposed suggestions with support practitioners. We identified opportunities for customer support to help survivors with care and precaution, such as by sharing tech safety resources and making external referrals. We provide recommendations for computer security companies to address tech-enabled IPV through customer support, including training frontline agents and building partnerships with IPV advocates. Based on this research, we have started providing respective training to partner companies. These ongoing early efforts underline the promise of computer security customer support as a feasible and necessary channel to help IPV survivors and potentially a broader range of tech abuse victims.

## Acknowledgements

We thank all participants for volunteering their valuable time and insights. We also thank Abraham Mhaidli, Alex Jiahong Lu, Jane Im, Tawanna Dillahunt, Yaxing Yao, and anonymous reviewers for constructive feedback on early drafts. Our work was partially supported by NSF grant #1916096, a NortonLifeLock Graduate Fellowship, and a Facebook Fellowship.

## References

[1] Substance Abuse and Mental Health Services Admin. Trauma training for criminal justice professionals, 2020. `https://www.samhsa.gov/gains-center/trauma-training-criminal-justice-professionals`.

[2] Kemal Veli Açar. Osint by crowdsourcing: A theoretical model for online child abuse investigations. *International Journal of Cyber Criminology*, 12(1):206–229, 2018.

[3] Budi Arief, Kovila PL Coopamootoo, Martin Emms, and Aad van Moorsel. Sensible privacy: How we can protect domestic violence survivors without facilitating misuse. In *Workshop on Privacy in the Electronic Society*, pages 201–204. ACM, 2014.

[4] Colorado Coalition Against Sexual Assault. Sexual assault advocacy & crisis line training guide, 2011. `https://www.ccasa.org/wp-content/uploads/2014/01/Sexual-Assault-Advocacy-and-Crisis-Line-Training-Guide.pdf`.

[5] Michael F Baber. *Integrated Business Leadership Through Cross Marketing*. Warren H. Green, 1986.

[6] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):210:1–210:27, 2021.

[7] Len Berry. Customer support services' next horizon: a commentary. *European Journal of Marketing*, 54(7):1805–1806, 2020.

[8] Michele C Black, Kathleen C Basile, Matthew J Breiding, Sharon G Smith, Mikel L Walters, Melissa T Merrick, Jieru Chen, and Mark R Stevens. National intimate partner and sexual violence survey: 2010 summary report. Technical report, National Center for Injury Prevention and Control, 2011.

[9] Mark Button, Lisa Sugiura, Dean Blackbourn, Richard Kapend, David Shepherd, and Victoria Wang. Victims of computer misuse: Executive summary. Technical report, University of Portsmouth, 2020.

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

[11] Nathan Collier. Mobile stalkerware: A long history of detection, 2019. https://blog.malwarebytes.com/android/2019/06/mobile-stalkerware-a-long-history-of-detection/.

[12] Veracities Public Benefit Corporation. Certified FETI | the official forensic experiential trauma interview, 2021. https://www.certifiedfeti.com/.

[13] Michelle Cottle. The adultery arms race, 2014. https://www.theatlantic.com/magazine/archive/2014/11/the-adultery-arms-race/380794/.

[14] Dana Cuomo and Natalie Dolci. Gender-based violence and technology-enabled coercive control in seattle: Challenges & opportunities. Technical report, TECC Whitepaper Series, 2019.

[15] Suzy D'Enbeau and Adrianne Kunkel. Domestic violence prevention and (mis)managed empowerment, 2013. https://www.natcom.org/communication-currents/domestic-violence-prevention-and-mismanaged-empowerment.

[16] Melissa E Dichter, Kristie A Thomas, Paul Crits-Christoph, Shannon N Ogden, and Karin V Rhodes. Coercive control in intimate partner violence: Relationship with women's experience of violence, use of violence, and danger. *Psych. of violence*, 8(5):596–604, 2018.

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

[18] Heather Douglas, Bridget A Harris, and Molly Dragiewicz. Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology*, 59(3):551–570, 2019.

[19] Jeff Elder. Google pulls stalker apps identified by avast, 2019. https://blog.avast.com/avast-identifies-stalker-apps.

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

[21] Women Against Violence Europe. Find help, 2020. https://www.wave-network.org/find-help.

[22] Centers for Disease Control and Prevention. Intimate partner violence, 2018. https://www.cdc.gov/violenceprevention/intimatepartnerviolence/index.html.

[23] Buffalo Center for Social Research. What is trauma-informed care, 2021. https://socialwork.buffalo.edu/social-research/institutes-centers/institute-on-trauma-and-trauma-informed-care/what-is-trauma-informed-care.html.

[24] Lorenzo Franceschi-Bicchierai. Kaspersky lab will now alert users to 'stalkerware' used in domestic abuse, 2019. https://www.vice.com/en_us/article/vbw9g8/kaspersky-lab-alert-stalkerware-domestic-abuse.

[25] Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth, and Sarah Tucker. The new age of stalking: Technological implications for stalking. *Juvenile and Family Court Journal*, 61(4):39–55, 2010.

[26] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "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):202:1–202:24, 2019.

[27] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):46:1–46:22, 2017.

[28] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise" How intimate partner abusers exploit technology. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 667:1–667:13, 2018.

[29] L Kevin Hamberger, Sadie E Larsen, and Amy Lehrner. Coercive control in intimate partner violence. *Aggression and Violent Behavior*, 37:1–11, 2017.

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

[31] Diarmaid Harkin, Adam Molnar, and Erica Vowles. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture*, 16(1):33–60, 2020.

[32] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *USENIX Security Symposium*, pages 105–122. USENIX Association, 2019.

[33] Nicola Henry and Anastasia Powell. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, & abuse*, 19(2):195–208, 2018.

[34] Safe Horizon. Tech safety: For victims of crime, abuse, domestic violence and stalking, 2016. https://www.safehorizon.org/wp-content/uploads/2016/06/1412609869_Tech-Safety-for-Victims-of-Abuse_Safe-Horizon.pdf.

[35] The National Domestic Violence Hotline. Domestic violence statistics, 2021. https://www.thehotline.org/stakeholders/domestic-violence-statistics/.

[36] The National Domestic Violence Hotline. The hotline, 2021. https://www.thehotline.org.

[37] NortonLifeLock Inc. Norton internet security center, 2021. https://us.norton.com/internetsecurity.

[38] Johns Hopkins University School Of Nursing. Empowering decisions for a safe path forward, 2021. https://www.myplanapp.org/.

[39] Carol E Jordan. Intimate partner violence and the justice system: An examination of the interface. *Journal of Interpersonal Violence*, 19(12):1412–1434, 2004.

[40] Jeanette Kerr, Carolyn Whyte, and Heather Strang. Targeting escalation and harm in intimate partner violence: Evidence from northern territory police, australia. *Cambridge Journal of Evidence-Based Policing*, 1:143–159, 2017.

[41] Amanda Kippert. Empowering survivors: Why domestic violence advocates say the best way to help survivors is to give them back control, 2015. https://www.domesticshelters.org/articles/escaping-violence/empowering-survivors.

[42] Richard A Krueger. *Focus groups: A practical guide for applied research*. Sage publications, 2014.

[43] Charity Lacey. The aftermath: the non-economic impacts of identity theft. Technical report, Identity Theft Resource Center, 2018.

[44] Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic, Bryan Ford, and Jean-Pierre Hubaux. On enforcing the digital immunity of a large humanitarian organization. In *Symposium on Security and Privacy*, pages 424–440. IEEE, 2018.

[45] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Designing Interactive Systems Conference*, pages 527–539. ACM, 2019.

[46] Roxanne Leitão. Technology-facilitated intimate partner abuse: A qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, 36(3):203–242, 2019.

[47] Karen Levy. Intimate surveillance. *Idaho Law Review*, 51(3):679–694, 2014.

[48] Karen Levy and Bruce Schneier. Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1):1–13, 2020.

[49] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 'internet of things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly*, 63:22–26, 2019.

[50] Eleanor Lyon, Jill Bradshaw, and Anne Menard. Meeting survivor needs through non-residential domestic violence services & supports: Results of a multi-state study. Technical report, National Resource Center on Domestic Violence, 2012.

[51] Malwarebytes. Malwarebytes lab, 2021. `https://blog.malwarebytes.com/`.

[52] Meghan L Marsac, Nancy Kassam-Adams, Aimee K Hildenbrand, Elizabeth Nicholls, Flaura K Winston, Stephen S Leff, and Joel Fein. Implementing a trauma-informed approach in pediatric health care networks. *JAMA pediatrics*, 170(1):70–77, 2016.

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

[54] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):72:1–72:23, 2019.

[55] David L Morgan. Focus groups. *Annual review of sociology*, 22(1):129–152, 1996.

[56] Albert Munanga. Cybercrime: A new and growing problem for older adults. *Journal of gerontological nursing*, 45(2):3–5, 2019.

[57] Christine E Murray, G Evette Horton, Catherine Higgins Johnson, Lori Notestine, Bethany Garr, Allison Marsh Pow, Paulina Flasch, and Elizabeth Doom. Domestic violence service providers' perceptions of safety planning: A focus group study. *Journal of Family Violence*, 30(3):381–392, 2015.

[58] Trauma & Mental Health National Center on Domestic Violence. A trauma-informed approach to domestic violence advocacy, 2011. `http://nationalcenterdvtraumamh.org/wp-content/uploads/2012/01/Tipsheet_TI-DV-Advocacy_NCDVTMH_Aug2011.pdf`.

[59] Northnode Inc. Domestic violence training for new staff & volunteers, 2008. `http://www.healthrecovery.org/images/products/34_full.pdf`.

[60] Global Network of Women's Shelters. Provide information, 2021. `https://www.gnws.org/index.php/women-s-helplines/provide-information`.

[61] A Parsu Parasuraman, Valarie A Zeithaml, and Leonard L Berry. Serqual: A multiple-item scale for measuring consumer perceptions of service quality. *Journal of Retailing*, 64(1):12–40, 1988.

[62] Melanie Randall and Lori Haskell. Trauma-informed approaches to law: Why restorative justice must understand trauma and psychological coping. *Dalhousie Law Journal*, 36:501–533, 2013.

[63] Melissa Rosen. 10 Customer Service KPI Metrics You Should Be Measuring (And How to Improve Them), 2021. `https://www.groovehq.com/support/customer-service-metrics`.

[64] Kevin Alejandro Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. The many kinds of creepware used for interpersonal attacks. In *Symposium on Security and Privacy*, pages 626–643. IEEE, 2020.

[65] Johnny Saldaña. *The Coding Manual for Qualitative Researchers*. Sage, 2015.

[66] Jillian R Scheer and V Paul Poteat. Trauma-informed care and health among LGBTQ intimate partner violence survivors. *Journal of Interpersonal Violence*, pages 1–23, 2018.

[67] Mahmood Sharif, Kevin Alejandro Roundy, Matteo Dell'Amico, Christopher Gates, Daniel Kats, Lujo Bauer, and Nicolas Christin. A field study of computer-security perceptions using anti-virus customer-support chats. In *Conference on Human Factors in Computing Systems*, pages 78:1–78:12. ACM, 2019.

[68] Suzanne M Slattery and Lisa A Goodman. Secondary trauma stress among domestic violence advocates: Workplace risk and protective factors. *Violence Against Women*, 15(11):1358–1379, 2009.

[69] Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Internet Measurement Conference*, pages 432–444. ACM, 2017.

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

[71] The Coalition Against Stalkerware. In short, 2021. `https://stopstalkerware.org/about/`.

[72] The Federal Trade Commission. FTC brings first case against developers of "stalking" apps, 2019. `https://www.ftc.gov/news-events/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps`.

[73] The Tails project. Tails is a portable operating system that protects against surveillance and censorship, 2021. `https://tails.boum.org/`.

[74] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, et al. Sok: Hate, harassment, and the changing landscape of online abuse. In *Symposium on Security and Privacy*. IEEE, 2021.

[75] The National Network to End Domestic Violence. Power & control wheel: On technology & abuse, 2006. `https://safechatsv.org/wp-content/uploads/2016/07/NNEDV_TechPowerControlWheel_Aug08.pdf`.

[76] The National Network to End Domestic Violence. Technology safety, 2021. `https://www.techsafety.org/`.

[77] Clinic to End Tech Abuse. Homepage, 2021. `https://www.ceta.tech.cornell.edu/`.

[78] Jenna Torluemke and Christine Kim. Nearly Half of Americans Admit to 'Stalking' an Ex or Current Partner Online, 2020. `https://www.businesswire.com/news/home/20200212005192/en/`.

[79] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *USENIX Security Symposium*, pages 1893–1909. USENIX Association, 2020.

[80] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during COVID-19. pages 71:1–71:17, 2021.

[81] The National Coalition Against Domestic Violence. State coalitions, 2020. `https://ncadv.org/state-coalitions`.

[82] Silvio Waisbord. Mob censorship: Online harassment of us journalists in times of digital hate and populism. *Digital Journalism*, 8(8):1030–1046, 2020.

[83] Lynette K Watts, Jessyca Wagner, Benito Velasquez, and Phyllis I Behrens. Cyberbullying in higher education: A literature review. *Computers in Human Behavior*, 69:268–274, 2017.

[84] Aslhey Weese and Dana Peiffer. Customer service: Then and now. In *Conference on User services*, pages 35–38. ACM, 2013.

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

[86] Georgia Zara and Sarah Gino. Intimate partner violence and its escalation into femicide. *Frontiers in Psychology*, 9:1777, 2018.

# A Focus Group Protocol: IPV Professionals

**Part 1: Introduction.** Thank you all for taking the time to talk to us. We're researchers from [institutions]. [Company] provides cybersecurity software and services like [products].

[Company] offers customer support hotlines and online chats to help their customers deal with tech-related issues. There are instances in which the caller appears to be in a dangerous situation, such as stalking and domestic violence. [Company] wants to better assist these callers and understand the appropriate scope for their customer support in doing so.

Today's meeting will be primarily discussion-based with a few activities. There are no right or wrong answers to any of our questions. We're simply interested in your opinions based on your own experiences or perspectives. You can choose not to comment and you can quit the session at any point.

We would also like to get your consent to audio record the workshop session as a backup of our notes. These will be transcribed, all identifying information will be removed, and we will destroy the original recordings once the transcription is done. Are you ok with us recording the meeting? Do you have any other questions before we get started?

- Let's go around the room with brief introductions. Please tell us your name, job title, and how many years you have been doing this job.
- Have you ever worked directly with clients? Have you encountered clients who have experienced IPV?
- Have you encountered clients who have experienced tech-related abuse? Can you give an example?

**Part 2: Presenting and Discussing Customer Support Scenarios.** Now we'd like to present a few example customer support transcripts and get your expert opinions on these interactions. These transcripts are based on real chats, but have been shortened and identifying information removed. We'll let you read each scenario and ask a few follow-up questions.

*IPV professionals' advice to this customer* Ignoring the technical aspect of this problem, imagine someone were to come to you with this problem:

- Are these problems similar to or different from the cases you normally receive at your organization? In what ways?
- What advice would you give based on the available information?

*IPV professionals' advice to the support agent* Now let's think about this customer's interaction with customer support...

- In your opinion, what could the customer support agent offer this customer beyond assistance with [product name]?
- Are there additional questions that customer support should be asking?
- Are there resources customer support could have shared?
- In your opinion, should customer support point to other organizations, such as shelters or the police? Why or why not? How might it be done?
- Should customer support provide specific advice about safety planning? Why or why not? How might it be done?

*Factors that might complicate advice* Let's discuss a few factors that make the situation trickier. For each case, should the support agent react differently in your opinion, why or why not?

- What if the agent thinks the attacker is recording/listening to the chat?
- What if the customer is not alone when the call takes place?
- What if the attacker could be calling to access a victim's account?

**Part 3: General Advice Going Beyond the Scenarios.** Now that we've looked at some examples of the problems that customer support gets, let's think about the broader role that customer support can play in providing support to victims of abuse.

- Under what circumstances, if any, do you think that customer support's duty to help extends beyond addressing product-specific issues identified by the customer?
- In your opinion, should customer support try to identify situations in which the caller may need additional safety planning advice? Why or why not? What can customer support do to identify such situations?
- Should customer support watch out for cues suggesting further questions are unsafe (e.g., due to monitored)? Why or why not?
- How should customer support respond if a customer reveals personal, sensitive information about an assault or suicide?
- What training or education do you think the support rep could have to help them avoid adverse outcomes? E.g., About IPV and risks related to leaving an abuser? About resources to share?

# B Focus Group Protocol: Support Agents

**Introduction.** We are conducting a research study around technology and intimate partner abuse. We are exploring how security companies can help IPV survivors through their customer support. So far we've conducted five focus groups with about 20 experts in this space, such as social workers and legal advocates, to collect their feedback on this topic. We now want to talk to you as customer support practitioners and security experts, to understand how effective, efficient, and practical some of these ideas are. After our talk today, we plan to develop recommendations from these insights and integrate them into guidelines and training materials for customer support agents, and we're happy to share them with you.

**Part 1: Study Background.** We conducted 5 focus groups with professionals to seek advice about how security companies can support IPV survivors. We presented three scenarios, created based on real chat transcripts from [Company], and asked participants how customer support could do better. The ideas we elicited from IPV professionals are not final. Participants sometimes disagreed with each other, and also mentioned the challenges and constraints of some of the ideas.

We'd like to ask some open questions about your organization:

- How is your customer support team organized?
- What are evaluation metrics for success for customer support agents?

We'd now like to ask about your experiences with IPV at your company.

- Have you or your employees encountered similar cases that involve IPV/technology abuse?
- What are your company's current efforts for supporting IPV survivors that you're aware of?

We will present our findings in four parts. During our presentation, please feel free to chime in whenever you have any questions or comments. At the end of each part we'll have a short summary and discussion to ask you some specific questions about what we shared with you and get your feedback. We expect each session to take about 12 minutes, and we'll leave a few minutes at the end of today's meeting to wrap up and discuss next steps.

**Part 2: Interacting with customers.** Suggestions from IPV professionals: • Explain why a product would be helpful • Avoid overpromising • Ask more probing questions

- What are your reactions to these suggestions? Comments or feedback?
- Do you think it is feasible?
- How much of this would you say is your team already doing?
- Would this create conflict with your evaluation metrics of support agents, such as the rate of "resolving issues?" If yes, Is there any way to mitigate such conflict?
- Do you see any challenges or concerns with these suggestions?
- Do you have ideas about how this could be done differently?

**Part 3: Advice given to customers.** What role do you think customer support should play in providing technical assistance vs. going beyond?

Suggestions from IPV professionals: • Discuss potential consequences of given advice • Provide resources for best security and safety practices

- What are your reactions to these suggestions? Comments or feedback?
- Have your employees already been discussing consequences of advice? If yes, could you give us an example?
- Are there downsides of discussing potential consequences of advice?
- What resources do your support agents refer customers to about security and safety practices? How often do they do this?
- Do you see any challenges or concerns with these suggestions?
- Do you have ideas about how this could be done differently?

**Part 4: Making referrals.** Suggestions from IPV professionals: • Refer customers to a specialized team within the company • Make external referrals based on trigger words

- What are your reactions to these suggestions? Comments or feedback?
- Do you already have a multi-tiered support system? What types of cases get transferred or escalated?
- How feasible do you think is it to have a specialized team within your company to deal with IPV/tech abuse?
- Do your support reps already refer customers to resources outside of the company? If yes, for what types of problems?
- From your experience, how difficult would it be to identify these cases? What are the challenges?
- Do you see any challenges or concerns with these suggestions?
- Do you have ideas about how this could be done differently?

**Part 5: Training materials.** Suggestions from IPV professionals: • Have agents be familiar with common tech abuse cases • Train agents for trauma-informed responses • Ensure the well-being of support agents

- What are your reactions to these suggestions? Comments or feedback?
- Have you embedded training for empathetic or trauma-informed responses in your current training materials/scripts?
- Are you already doing anything to prepare agents to handle difficult / traumatic customer issues?
- What have you done to ensure the well-being of your employees? Could anything be done better?
- Do you see any challenges or concerns with these suggestions?
- Do you have ideas about how this could be done differently?

**Closing.** We want to use the insights from our work with IPV experts and customer support teams, like you, to develop guidelines and training materials for integrating IPV support into customer support. If you're interested, we will share materials with you when we have drafted them.

# C Focus Group Analysis Codebook

We provide our codebook in the following format: **category (counts of belonging codes):** *a list of codes*.

## C.1 IPV Professionals

**Advice to IPV survivors (3):** *adopt good security practices, document evidence, replace compromised devices* • **Advice on agent-customer interaction (10):** *avoid overpromising, avoid assumptions of IPV, avoid victim blaming, ask questions to better diagnose the situation, ask about the customer's top concern, explain how the product solves existing problems, give the customer decision-making agency, make disclaimers about the advice's consequences, role in safety planning, use more empathetic language* • **Advice on customer support coordination (10):** *build long-term relationships with the customer, change the evaluation metrics, refer to a specialized team, refer to external resources, refer to IPV advocacy organizations and hotlines, refer to law enforcement, refer to legal experts, refer to trafficking-specific resources, responsibilities of the IPV-specialized team, track the scale of cases* • **Advice on customer support training (4):** *trauma-informed responses, capture red flag words, assess the situation, know common forms of tech abuse* • **Challenges of customer support (8):** *advice may create additional danger, loop between IPV advocates and tech companies, complex structure of existing resources, go overboard with asking questions, issues in transferring calls, make assumptions of IPV victim status, pressure of getting things done, support agents might overreact* • **Negative aspects of customer support (5):** *dismissive language, give a false sense of security, no trauma-informed responses, responses too product-focused, responses too script-based* • **Positive aspects of customer support (2):** *ask open-ended probing questions, use empathetic language* • **Adverse scenarios: advice on customer support (7):** *be vague in calling back, check if line is secure, do not ask for PII, explain potential risks, redirect to another phone, spot red flags for impersonation, verify customer's identity* • **Adverse scenarios: challenges of customer support (2):** *advice tips off abuser, limited channels for communication* • **Miscellaneous (9):** *participants' job roles, participants' experience with tech abuse cases, adverse scenarios are rare, coalition between tech companies and advocates, connection between IPV and human trafficking, ensure the well-being of support agents, generational divide in interacting with mobile devices, provide free services for IPV survivors, shared responsibility between tech companies*

## C.2 Customer Support

**Challenges to suggestions (14):** *an independent team may not be feasible, infrequent IPV cases mean they'll be mishandled, agents are international, concern about sharing correct resources, uncertainty about ability to help, unqualified or untrained agents could cause problems, scripting could lead to overpromising, identifying survivors is challenging, customer support is already overworked, uncertainty about successfully identifying tech in IPV, stalkerware might be dual-use, attacker might be listening to support conversation, training will need to be regular, agents can't make the customer take the suggested action* • **Suggestions that already exist (7):** *asking probing questions & not overpromising, escalating unusual cases to experts, sharing external resources, providing general tech best-practices to customers, using empathetic language, hosting resources on stalkerware, escalation team is familiar with IPV* • **Supportive comments (10):** *making agents aware of IPV is worthwhile, IPV survivors need specialized advice, all agents should be trained on IPV, agents also need support when handling IPV cases, empathetic language helps everyone, agents should ask more questions to avoid overpromising, adding additional external referrals is achievable, having a dedicated team for IPV cases is good, training agents on IPV is good, agents should consider ramifications of their advice* • **Comments on how participants or company think about the problem (Values) (6):** *customer satisfaction is a priority, trust among agents is important, the product is the agent's primary responsibility, customer needs to have confidence in their tech, the product is a solution, need to balance accuser's v abuser's rights* • **Agents' metrics for evaluation (4):** *customer satisfaction, throughput, minimizing open cases, quality assurance review* • **New ideas for addressing the problem (6):** *create company-wide awareness campaign, create new resources for customers, track number of IPV cases, make training story-based, create a standard operating procedure for IPV customers, provide basic digital training to customers* • **Miscellaneous (2):** *participant shared tech advice, participant shared a story about supporting a customer*