"It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse*

Sophie Stephenson†, Majed Almansoori†, Pardis Emami-Naeini‡, Rahul Chatterjee†
†*University of Wisconsin—Madison,* ‡*Duke University*

Abstract

Victim-survivors of intimate partner violence (IPV) are facing a new technological threat: Abusers are leveraging IoT devices such as smart thermostats, hidden cameras, and GPS trackers to spy on and harass victim-survivors. Though prior work provides a foundation of what IoT devices can be involved in intimate partner violence, we lack a detailed understanding of the factors which contribute to this *IoT abuse*, the strategies victim-survivors use to mitigate IoT abuse, and the barriers they face along the way. Without this information, it is challenging to design effective solutions to stop IoT abuse.

To fill this gap, we interviewed 20 participants with firsthand or secondhand experience with IoT abuse. Our interviews captured 39 varied instances of IoT abuse, from surveillance with hidden GPS trackers to harassment with smart thermostats and light bulbs. They also surfaced 21 key barriers victim-survivors face while coping with IoT abuse. For instance, victim-survivors struggle to find proof of the IoT abuse they experience, which makes mitigations challenging. Even with proof, victim-survivors face barriers mitigating the abuse; for example, mitigation is all but impossible for victim-survivors living with an abusive partner. Our findings pinpoint several solutions to combat IoT abuse, including increased transparency of IoT devices, updated IoT access control protocols, and raising awareness of IoT abuse.

1 Introduction

Everyday technologies are being (ab)used as tools for *intimate partner violence* (IPV). For victim-survivors of IPV, an increasing technological threat comes from special-purpose, Internet-connected devices, also called *IoT devices*. Abusers leverage Internet-connected video doorbells and home security cameras to spy on their partners [32], use smart thermostats to turn off the heat in the winter [20], and track victim-survivors with hidden AirTags [1,22,41,44]. This IoT-enabled abuse, or *IoT abuse*, is concerning as these IoT devices can have unprecedented control over the victim-survivor's home environment, including security systems, physical access controls, and other safety measures.

An emerging research effort has begun to investigate IoT abuse in IPV. For example, through workshops with victim-survivors, Leitão [38] found that victim-survivors worry that their abusers will repurpose home security systems for surveillance. In another study based on interviews with advocates, Tanczer et al. [61] outlined the pervasive and harmful nature of IoT abuse; they found that abusers misuse video doorbells, cameras, thermostats, and baby monitors to spy or harass victim-survivors and can use them to *gaslight* a victim-survivor by "denying facts, the environment around them, or their feelings." Tanczer et al. also identified some barriers that victim-survivors face when handling IoT abuse. For example, abusers often set up IoT devices in the home, meaning it is difficult to revoke their access.

These works provide the security community with a foundational understanding of IoT abuse in IPV and underscore some of the challenges victim-survivors and advocates face. However, we lack an in-depth understanding of *how* and *why* IoT abuse occurs. Specifically, how do victim-survivors realize that IoT abuse is happening, how do they cope with the abuse, and why is IoT abuse difficult to mitigate? Given IoT devices' dangerous predisposition to cause harm, it is critical that we understand these aspects of IoT abuse.

In this work, we investigate *how* IoT abuse occurs in IPV and *why* it is difficult to mitigate with three research questions:

RQ1: How do IPV victim-survivors identify IoT abuse?

RQ2: What strategies do victim-survivors and advocates use to mitigate IoT abuse?

RQ3: What barriers do victim-survivors and advocates face in identifying or mitigating IoT abuse?

The nuances of IoT abuse in IPV cannot be deduced from work on general tech abuse. IoT abuse is unique in several ways. First, unlike mobile phones or online accounts which are primarily personal, IoT devices are designed to be shared; second, IoT devices are situated in victim-survivors' physical

*This paper was published in USENIX Security 2023.

environment such as their home or vehicle; and third, unlike malicious apps on a mobile phone, IoT devices are not monitored or controlled by a single overarching entity. Moreover, because of the novelty and technical complexity of IoT devices, victim-survivors and advocates are less familiar with IoT devices and how they can be abused. Because of these differences, we need to analyze real-world accounts of IoT abuse to gain a deeper understanding.

Thus, in this paper, we interview 20 participants who have either supported victim-survivors experiencing IoT abuse (17 participants) or experienced IoT abuse firsthand (3 participants). Our findings expand the community's understanding of IoT abuse and indicate necessary interventions. First, we surface 39 real-world instances of IoT abuse involving various types of IoT devices, including outdoor security cameras, indoor cameras, GPS trackers, thermostats, smart lights, and more. By discussing these instances, we raise awareness of IoT abuse in the community and confirm several hypotheses from prior work [38, 39, 46, 61].

We also establish a number of approaches that victim-survivors take to identify and mitigate IoT abuse, as well as 21 specific barriers they face. For example, victim-survivors have a difficult time proving that IoT abuse is occurring because (1) IoT devices rarely indicate abusive behavior and (2) it is difficult to find hidden surveillance devices, such as hidden cameras and GPS trackers. Even if victim-survivors find ways to identify IoT abuse, mitigating the abuse is particularly challenging for victim-survivors who are living with abusive partners. On the support system side, advocates struggle to assist victim-survivors due to a lack of training in IoT abuse and a dearth of resources that they can refer to. Victim-survivors sometimes reach out to (or are referred by advocates to) outside services, such as car mechanics or network providers, but rarely receive satisfactory support because these services are not trained in IoT abuse or trauma-informed care.

These findings reveal an urgent need for interventions. Towards combating IoT abuse, we propose a suite of challenges for future work, including redesigning IoT devices to help identify abusive behavior, designing tailored tools and services for mitigating IoT abuse, raising awareness of IoT abuse across support services and the broader public, and collaborating with legal experts.

2 Background & Related Work

Intimate partner violence (IPV)—"physical, sexual, or psychological harm by a current or former intimate partner or spouse" [8]—is a pervasive problem in the United States [58] and globally [7]. In this paper, we refer to people who have experienced IPV as *victim-survivors*. This is an inclusive term which accounts for the variety of ways people understand and cope with their experiences of abuse [21, 56].

Following prior work [29, 30, 56, 61, 64, 66], we primarily learn about victim-survivors' experiences by talking to their *advocates*. Advocates support victim-survivors during and after their experience with IPV by safety planning, providing advice, accompanying them to court or other appointments, directing them to related services, and above all, empowering the victim-survivor to do what is best for them. Advocates have a unique view of both broad patterns of IPV (by working with many clients at once) as well as deeper details of individual cases (by engaging with clients often and over a long period of time).

2.1 Intimate Partner Violence and Technology

Unfortunately, more and more intimate abusers have begun to use technology against their partners. Technology abuse in IPV—referred to in this paper as *tech abuse*—comes in many forms. In some cases, abusers use tailor-made spyware apps to spy on their partners' messages, location, calls, and other private data [15, 24, 50, 62]. However, tech abuse most commonly involves less sophisticated methods. For example, abusers use a victim-survivor's accounts to spy on their communications and private data, post intimate images without consent, or block them from accessing their accounts [29, 66]. Using these methods, abusers can assert *digital coercive control* [33] over victim-survivors.

Tech abuse is difficult to address because it is situated in a complex context [25, 29, 30, 37, 42, 56, 61, 66]. For one thing, intimate partners often share access to accounts and devices, which gives abusers nearly ubiquitous access to digital assets [29, 30, 47]. Further, IPV can persist over many years, and victim-survivors' needs can change over time. For example, while living with an abusive partner, victim-survivors often limit technology use to avoid surveillance; in contrast, after leaving, victim-survivors may focus on severing digital ties and hiding their new life from the abusive partner [42, 56].

To counteract tech abuse, therefore, security researchers have worked to build tailored *clinical computer security* [28, 34] solutions which provide direct support to victim-survivors [28, 34, 63, 64]. Others have worked to inform these efforts by studying the existing support practices used by advocates [56, 61] and customer support services [71] when addressing tech abuse. Though these measures do not erase tech abuse entirely, they have been a valuable resource for victim-survivors [63].

2.2 Intimate Partner Violence and IoT Devices

This paper targets *IoT abuse*, a subset of tech abuse involving IoT devices. IoT devices include smart home devices—such as smart light bulbs, thermostats, door locks, cameras, and video doorbells—as well as other connected devices like GPS trackers, Bluetooth item finders (e.g., AirTags [1]), and smart vehicles. These devices are predisposed to cause harm when used maliciously. First, IoT devices exist in intimate settings, such as the home, car, or among physical possessions. A malicious user of IoT devices can therefore access sensitive data

about a person's activity in proximity to their home and possessions or control their environment. Further, in-home IoT devices are often meant to be shared with multiple users, which can cause power and control struggles. For example, Geeng and Roesner [31] found that the person who installs devices has the most control over them and may purposefully restrict access from other residents. Unfortunately, unlike the mobile or computer operating systems in the case of spyware [15, 24], there is no centralized authority to control or monitor all IoT devices in the vicinity, making it harder for a victim-survivor to identify misuse or take back control.

Today, IoT devices are routinely misused for spying and harassment, including in IPV scenarios [43]. News articles report that abusers use IoT devices to change the temperature, flicker smart lights, blast music, or turn the TV on and off in the victim-survivor's home as a form of psychological abuse [20, 32]. Others have reported that abusers use AirTags [1] and cameras to spy on intimate partners' location or other activities [22, 32, 41]. Despite these urgent concerns, the majority of academic work on IoT security fails to recognize the threat that IoT devices can pose in IPV contexts [55].

To learn more about this phenomenon, recent academic work has used several methods to characterize IoT abuse. Scholars have surveyed IoT-related "intimate threats" [39], leveraged a usability assessment to detect the potential for IoT abuse [46], anticipated IoT threats with victim-survivors [38], and investigated the covert spy devices for sale on large online retailers [23]. Most recently, Stephenson et al. [59] gathered online accounts of IoT abuse and defined four *abuse vectors*, or patterns that IoT abuse follows. For example, in the Covert Spying vector, abusers spy on victim-survivors using hidden IoT devices such as spy cameras, audio recorders, and GPS trackers. These preliminary works lay out the *types* of IoT abuse which can occur (via smart speakers, home security systems, baby monitors, and more), but do not provide insight into the more nuanced dynamics of IoT abuse in practice.

An emerging research effort led by the Gender and IoT (G-IoT) team at UCL has dug deeper into IoT abuse [40, 57, 60, 61]. As part of a larger interview study on tech abuse, Tanczer et al. [61] found several cases involving cameras, doorbells, smart speakers, baby monitors, and smart watches and outline a few barriers victim-survivors face when dealing with IoT abuse. Towards prevention, the G-IoT team has called for solutions such as raising awareness, updating legislation, and coordination between the security community and IPV advocacy groups [40, 60]; concretely, Slupska and Tanczer demonstrated how threat modeling could be used to reveal opportunities for IoT abuse [57].

Although the research community has begun to investigate IoT abuse, we lack an in-depth understanding of how and why IoT abuse takes place in IPV situations. In this study, we add to this emerging research effort by talking to advocates and victim-survivors who have seen or experienced IoT abuse. From their firsthand and secondhand accounts, we gain insights into the types of IoT abuse that occur (Section 4), victim-survivors' and advocates' experiences coping with IoT abuse (Sections 5–6), and how we can remove barriers from the mitigation process (Section 7).

3 Interview Procedures & Data Analysis

Under the guidance of local victim service providers (VSPs), we performed interviews with 20 participants. Seventeen participants (IDs A1–A17) are advocates—case managers, technology consultants, program coordinators within VSPs, VSP directors, and attorneys—who have worked with victim-survivors experiencing IoT abuse. In addition, three participants (VS1–VS3) are victim-survivors who have experienced IoT abuse firsthand. In total, these participants told us about 39 unique instances of IoT abuse (summarized in Fig. 4).

3.1 Ethical Considerations

We recognize the sensitive nature of these interviews and the risks participants may undertake by discussing their experiences with us. Though this study was approved by our IRB, we took additional measures to avoid causing harm to participants, in part guided by [18]. We took a trauma-informed approach [65] to designing our interview protocols and consulted with VSP leaders to ensure that our study would not place any unintentional burden on participants or retraumatize them. We handled interview recordings and transcripts with care: we removed all identifying information from transcripts, deleted audio recordings as soon as possible, and stored all study data in a private repository accessible to only the study researchers. We did not collect signatures from participants, as this would be the only document linking them to the study. Finally, we report only aggregate demographics.

Though we interviewed most participants individually, we also ran one focus group for advocates at VSP7 (Section 3.3). Focus groups generally present a higher risk of data leakage because participants discuss the study topics together and may share sensitive information outside the group. However, because this was an interview exclusively with advocates from a single organization, we feel there was no additional risk of data leakage. As three of the authors have observed from their work as tech abuse consultants (Section 3.4), advocates frequently discuss and collaborate on clients' cases within their VSP; our focus group, therefore, is similar to the discussions which already happen within the VSP.

3.2 Recruitment

We recruited participants from eight VSPs in the USA (Fig. 2). To be eligible for the study, participants had to be over 18 years old and be either a victim-survivor of IoT abuse, or an advocate who has worked with clients experiencing IoT abuse. At the outset of the study's, we asked leaders of multiple VSPs in a Midwestern city to advertise our study to their staff and clients. Some advocates reached out to us directly to

Role		Role type		Years advocacy		Age		Gender		Race/Ethnicity	
General advocate	2	Full-time	16	<2 years	1	18-24 years	1	Woman	18	Asian	1
Legal advocate	13	Volunteer	1	2-5 years	4	25-34 years	8	Man	1	Black or African American	1
Tech advocate	2	N/A	3	6-9 years	6	35-44 years	6	Non-binary	0	Hispanic or Latino	3
VSP leader	4			10+ years	6	45-54 years	1			Native Hawaiian/other Pacific Islander	1
Client	3			N/A	3	55-64 years	1			White	15

Figure 1: Aggregate demographics for our 20 participants. To protect participant privacy, we do not share specific demographic information about any individual participant and simplify role titles for further anonymity. Participants may fall into multiple categories, e.g., take on multiple roles at a VSP. One participant chose not to fill out our demographic form.

ID	VSP1	VSP2	VSP3	VSP4	VSP5	VSP6	VSP7	VSP8
# Ppts	6	2	1	1	1	1	7	1
Region	MW	NE	MW	MW	MW	MW	MW	MW

Figure 2: Our participants were associated with eight victim service providers (VSPs) in two regions of the US: the Midwest (MW) and Northeast (NE).

participate; some were suggested to us by earlier participants, and we contacted them individually to advertise the study. We also reached out to three tech clinics [34] in the USA to advertise the study. Three authors work directly with victim-survivors, so we also advertised the study to victim-survivors after routine tech abuse consultations.

3.3 Semi-Structured Interviews

We designed two semi-structured interview protocols: one to learn from advocates' experiences helping clients with IoT abuse, and one to learn about victim-survivors' personal experiences with IoT abuse.[1] We piloted the procedures internally and sought advice from outside experts, including VSP leaders, to ensure that our interviews would not harm or re-traumatize our participants [18].

For each IoT abuse incident the participant could recall, we asked about the smart devices that were involved in the incident, how those devices were weaponized, how the victim-survivor detected and/or attempted to mitigate the abuse, and contextual details surrounding the abuse incident (e.g., whether the victim-survivor and the abuser were living together). For advocates, we also inquired about the advocates' preparedness for these types of cases and their strategies for helping clients. We did not explicitly ask what training advocates received. Finally, we asked participants about their general perceptions of smart devices and their recommendations for others facing IoT abuse.

During the interviews. We interviewed participants between June 2022 and April 2023. Nine interviews were conducted in-person and eleven took place over Zoom. At the start of each interview, we showed participants an information form and asked for their verbal consent to participate. We also asked for their consent to record the interview; if granted, we recorded the interview audio using Otter.ai [14]. To help participants think of relevant cases, we showed participants a visual aid with photos and names of several common smart devices.

The first author primarily led the hour-long interviews while a second author took detailed notes. During interviews, we addressed all prepared questions, but allowed space for extra discussions and tangents as they arose. At the end of each interview, we collected demographic information (Fig. 1) by having the participant fill out an anonymous Google Form. All demographic questions were optional. We compensated victim-survivors with $20 for their time [18]; leaders at one VSP suggested we did not need to compensate advocates who participated in our study, which reflects prior work [30].

Focus group. At VSP7, some advocates requested to be interviewed as a group. Thus, A11–A14 participated in an in-person, 1.5-hour-long focus group instead of individual interviews. This procedure was similar to the individual interview procedure, with a few changes. To streamline the interview, we asked introductory questions about each advocate's role, experience, and opinions about smart devices in a pre-focus-group survey. During the focus group, we first asked participants to brainstorm relevant cases using worksheets we distributed. Participants shared relevant details about each case with the group; then, the first author led participants in a discussion about the cases.

3.4 Data Anonymization & Analysis

Immediately after each interview, we cleaned and anonymized the automated Otter.ai interview transcript by correcting any errors and removing any references to personal information—names, locations, companies, universities, unique word choices, etc. Once the transcript was ready, we destroyed the audio recording.

Coding process. To analyze the interviews, we used structural coding [52], a good fit for interview studies [17, 45]. First, the first author created twelve structural codes based on our research questions (e.g., *identifying IoT abuse*). The same coder then analyzed the first three interview transcripts and generated sub-codes. All authors discussed this preliminary codebook, resolved disagreements, and updated the codebook

[1] Our interview procedures, handouts, and codebook are available at https://go.wisc.edu/gh813r.

Term	a few	some	about half	most	almost all	all
# Ppts	1–4	5–8	9–11	12–15	16–19	20

Figure 3: Terminology we use to indicate the frequency of different themes in Sections 4–6.

accordingly. Then, two coders analyzed another interview with this codebook, resolved disagreements between them, and discussed the changes with the full group once again.

With this solidified codebook, two coders divided and coded each of the 20 interviews. We employed *collaborative qualitative data analysis* (CQA) [49], which involved meeting regularly to discuss confusions, share emerging themes, and update the codebook as needed. This data analysis methodology provides the validity of collaborative coding without the need for inter-coder reliability, since the coders iteratively discuss to reach a consensus during analysis [49].

Capturing instances of IoT abuse. While coding, we made a list of each instance of IoT abuse that our participants discussed. We defined an *instance* of IoT abuse as a tuple of the victim-survivor, the IoT device involved in the abuse, and the type of abuse (e.g., surveillance vs. harassment). In total, our study participants mentioned 39 unique instances of IoT abuse. Fig. 4 summarizes the different instances of IoT abuse that were discussed in our interviews, as well as general patterns advocates have observed.[2]

Positionality statement. Since qualitative research designates "the researcher as the data collection instrument" [19], our work is influenced by the identities and experiences of the authors [16, 18]. Two authors are women, and two are men. None of the authors have personally experienced IPV, and we acknowledge our understanding of IPV is only as observers. However, three authors are trained on IPV advocacy and trauma-informed care, and regularly volunteer as tech abuse consultants to help victim-survivors identify and mitigate tech abuse happening through mobile phones and online accounts. This experience helps us conduct the study with care and understand the nuances of tech abuse.

Terminology. This is a small-scale qualitative study, meaning that the specific frequency of codes or themes may misrepresent the importance of our findings. Thus, in Sections 4–6, we use the keywords in Fig. 3 to refer to different numbers of participants (as was done in [27]).

3.5 Limitations

Our small participant pool is the main limitation of this work. It was difficult to find participants who had experienced IoT abuse or helped clients experiencing IoT abuse. IoT abuse is yet to be as prevalent as other forms of tech abuse [61], and victim-survivors often cannot find proof that IoT abuse is occurring (as we discuss in Section 5). In any case, our results may be limited to the locations and communities we capture; i.e., primarily White women in the Midwestern USA (Fig. 2, Fig. 1). More work should be done to identify the specific barriers facing marginalized populations, such as victim-survivors of color and LGBTQ+ victim-survivors, who are coping with IoT abuse globally.

Additionally, only 3 of the participants have themselves experienced IoT abuse. The 17 advocates could only share a secondhand perspective, but they were still able to provide valuable information about specific cases they have worked on, as well as general trends they have observed. These advocates' years of experience—over 148 years in total, or 8.7 years on average—give them a wealth of accumulated knowledge of IoT abuse and other forms of tech abuse, even if they have not themselves experienced it [56]. We follow other key works which learned from the experiences of advocates [29, 30, 56, 61, 64, 66].

Finally, like many interview studies, we are limited by recall bias (i.e., participants may not accurately recall all details of their experiences). We also assume that participants accurately discuss legal topics (Section 6.4), since we do not have the legal expertise to evaluate their claims.

4 Characterizing IoT Abuse

IoT abuse can take many forms. Our participants recounted 39 specific instances of IoT abuse along with general patterns of IoT abuse they have noticed in their work. Here, we summarize the different types of IoT-enabled abuse captured by our interviews (Fig. 4). Several of these types of abuse have been hypothesized [38, 39, 46, 48] or reported [40, 47, 60, 61] in prior work, and we add to this discussion by providing real-world examples of IoT abuse. Our primary contribution, however, lies in our nuanced analysis of these cases which surfaces the thought process of victim-survivors and advocates when dealing with IoT abuse (Sections 5–6).

4.1 Types of IoT Abuse

Audio/video surveillance. Almost all interviews mentioned some form of audio/video surveillance via cameras, video doorbells, and baby monitors. There were three distinct patterns in this type of abuse. First, when abusers and victim-survivors were living together, abusers spied on victim-survivors using known, shared cameras in the home. Sometimes these cameras were purchased with the consent of both the abuser and the victim-survivor for a purpose such as keeping an eye on a child or pet; other times, the shared cameras were purchased without the consent of the victim-survivor. The second type occurred when the abuser had left the shared home (sometimes due to a restraining order), but retained

[2] More details about each instance of IoT abuse are available at https://go.wisc.edu/gh813r. We provide only an overview of each instance and do not include any potentially identifying details.

Type of abuse	Specific pattern	Interviews	#
Audio/video surveillance	Abusers place **hidden cameras** inside a survivor's home in order to spy on them. They sometimes additionally post footage from these cameras online.	VS3, A1, A2, A3, A6, A8, A10, A11, A12, A13, A14, A15, A17	13
	Abusers spy using **cameras**, **video doorbells**, and **baby monitors** which are known to the survivor. The cameras are often purchased for a legitimate reason and/or with the survivor's consent.	VS2, A1, A3, A4, A6, A7, A11, A12, A13, A14, A16	11
	After the abuser leaves a shared household, they retain access to **known cameras** or **video doorbells** and use that access to spy.	VS2, A5, A7, A11	4
Location tracking	Abusers hide **tracking devices** such as AirTags, GPS trackers, and Bluetooth earbuds in cars, bags, and toys.	VS3, A1, A3, A4, A5, A7, A8, A10, A11, A12, A13, A14, A15, A17	14
	Abusers use the activity logs/notifications from **home access control systems** (security systems, garage door openers) as well as **smart appliances** (motion-activated smart lights) to track the survivor's movement in and around the home.	VS1, VS2, A1, A3, A5	5
	Abusers use the provided apps for **smart cars** to track a survivor's location via the car.	A9	1
Data tracking	Abusers monitor survivors' activity and data on **smart home devices** (e.g., smart TV, router, smart speaker).	VS2, A3, A10	3
Environmental harassment	Abusers manipulate **smart home devices**, including thermostats, lights, smart TVs, smart speakers, and baby monitors, to disturb the survivor's home environment.	VS2, A4, A5, A4, A7, A10, A17	7
Access restriction	Abusers disconnect or block a survivor's access to certain **IoT devices** in order to isolate or annoy the survivor. They also use **smart locks** to block access to the house.	A1, A17	2

Figure 4: The types of abuse the victim-survivors (VS#) and advocates (A#) have seen or experienced.

access to cameras inside or outside the home. The third type happened when the abuser placed hidden cameras inside the home of the victim-survivor without their knowledge. Sometimes, especially with hidden cameras, abusers shared the intimate images and videos of the victim-survivor online.

Location tracking. Location tracking was also mentioned in almost all interviews. Abusers placed hidden tracking devices such as Apple AirTags, GPS trackers, or even Bluetooth earbuds inside victim-survivors' cars to track their location. Abusers also placed tracking devices in bags and toys, though this was a less common tactic. In one case, a tracking device was not necessary; the abuser leveraged the app associated with the victim-survivor's smart car to track its location. While tracking a survivor's location, abusers sometimes targeted additional stalking or harassment towards other people in the vicinity, such as law enforcement or family members.

For more geographically-restricted location tracking, abusers used the activity logs of smart home devices. For example, abusers with access to a smart garage door opener or a home security system could tell when the garage door opened or the alarm system was turned off, revealing when the victim-survivor left or arrived home. Abusers also learned this information from motion-activated appliances such as smart lights. VS1 felt trapped by this type of surveillance: "*With cameras, with the garage door, and the alarm system, all that, it's the equivalent of feeling like you're in jail.*"

Data tracking. In a few cases, abusers used access to victim-survivors' smart home devices to keep track of data points like watch history on a smart TV, browsing history, and calendar information. This invasion of privacy also led to other forms of abuse: in one case, the abuser used a smart speaker to tell when the victim-survivor would be at the grocery store, then confronted them at the store.

Environmental harassment. With smart home devices, abusers can create disruptive and harmful changes to the home environment. Our participants told us how abusers had used smart home devices to flicker lights, change the temperature, play content on a TV, talk through a speaker, and change the background on smart hubs and TVs to the victim-survivor's nude photos. These environmental disruptions sometimes had dire consequences including added physical, financial, and psychological abuse. For example, in one case, flickering smart lights prevented the victim-survivor from sleeping and fluctuating temperatures increased their energy bill.

Access restriction. Finally, abusers used smart home devices to restrict a victim-survivor's access to resources (like the internet) or support systems. One abuser did this by disconnecting the victim-survivor's IoT devices to prevent them from seeking help; another changed the Wifi password to prevent the victim-survivor from accessing the internet. One abuser also locked the victim-survivor out of their own home by changing the code on the previously-shared smart lock.

4.2 Stages of IoT Abuse

Through these varied instances of IoT abuse, we identified three main stages in the way victim-survivors experience IoT abuse: *Suspecting IoT Abuse*, *Identifying IoT Abuse*, and *Mitigating IoT Abuse*. As Fig. 5 shows, victim-survivors can move between these stages in multiple directions, which adds to the complexity of IoT abuse.

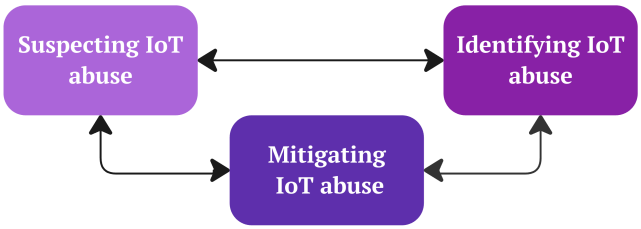

Figure 5: The basic stages of IoT abuse we observed.

Suspecting IoT Abuse. In this stage, victim-survivors suspect that their partner is using IoT devices against them. Often, they become suspicious due to actions from their abuser which indicate surveillance—e.g., the abuser knows things they shouldn't.

Identifying IoT Abuse (Section 5). In this stage, a victim-survivor identifies how abuse is happening or tries to validate their suspicions. This can take two forms. If the abuser is using *hidden* IoT devices for abuse, the victim-survivor needs to find those devices. Otherwise, if the abuser is using *known* IoT devices, the victim-survivor needs to identify which devices are being misused. Sometimes (maybe due to barriers to identification), victim-survivors skip this stage entirely and go straight to mitigations. Other times, victim-survivors unintentionally identify that IoT abuse is happening without any prior suspicion—for example, in one case, a victim-survivor noticed a hidden camera in their apartment because its low-battery light was on. In these cases, victim-survivors start at *Identifying IoT Abuse* without *Suspecting IoT Abuse*.

Mitigating IoT Abuse (Section 6). In the last stage, victim-survivors try to mitigate the IoT abuse they are experiencing. We will discuss two categories of mitigations: mitigations victim-survivors attempt themselves, and strategies advocates use to help victim-survivors mitigate the abuse. Though there appear to be many mitigation options for victim-survivors, there are also many barriers to attempting these options; for one thing, mitigations can ultimately lead to more abuse.

5 Identifying IoT Abuse

When dealing with these varied forms of IoT abuse, the first step many victim-survivors take is identifying the abuse. This can mean investigating known devices, looking for clues that the devices are being used maliciously; it can also mean finding hidden IoT devices which are being used for surveillance. If victim-survivors can pinpoint how IoT abuse is happening, mitigating the abuse is an easier task—unfortunately, the barriers we will discuss in this section (`B1`–`B6`) prevent many victim-survivors from identifying abuse at all.

5.1 Identifying Abuse with Known Devices

In most interviews, participants told us how identifying that known devices are being used maliciously starts with a simple process of elimination. Victim-survivors notice that abusers know things they should not, such as private conversations that occurred in the home. Then, they wonder: "*How is it possible that they know? [...] 'Oh, we have a camera.*'" (A1). This logic is often enough to confirm suspicions.

A few participants discussed how victim-survivors investigated further by manually looking through a device's settings. For instance, VS2 "*looked up and dug deeper into the settings for the Ring [Doorbell] and found that he had his smartphone as an authorized device.*" Similarly, a few described how victim-survivors asked outside services for help investigating their devices. For instance, victim-survivors investigated routers with help from tech-savvy neighbors and Wi-Fi technicians.

When trying to identify that IoT abuse is happening, victim-survivors face two major barriers.

`B1`: IoT devices do not indicate abuse. Most participants described a case where IoT abuse was *obvious* to the victim-survivor, but the IoT devices themselves did not offer any proof of the abusive behavior. A1 expressed frustration on behalf of one such victim-survivor, whose partner was harassing her with a smart thermostat: "*Does she know it was him? Does she have proof that it was him? No. But who else has that control?*" (A1). In particular, devices typically do not provide activity logs or notifications, such as "*This username is changing the temperature*" (A4), which could help pinpoint abusive activity. Further, if the victim-survivor and the abuser share the device, the abuser can easily delete proof of surveillance. For this reason, VS2 had trouble confirming that their partner was spying through the Ring Doorbell, even though the doorbell keeps logs of live viewing activity: "*If he deleted [the log] after he recorded that, before I got back from wherever I was going, I wouldn't know*" (VS2).

`B2`: IoT devices are not seen as a threat. About half of the participants noted that IoT devices can fade into the environment, meaning victim-survivors might not consider they could even be used for abuse. As A13 puts it, "*While I see cameras used so much more, it's less alarming to victims I work with than like, finding a GPS tracker on their car [...] The camera is like hidden in plain sight*" (A13). One reason for this is "*it's always been there, and it's always worked when you need it to work*" (A1). Prior research has shown that users regularly underestimate security threats with IoT devices [67, 69]; in IPV, this lack of awareness can prevent victim-survivors from considering their IoT devices as risky.

Additionally, some participants noted that abusers lie about misusing IoT devices. VS2 noted that their abusive partner lied about *access* to the shared Ring Doorbell. This eased their mind about the doorbell and made it even more difficult to pinpoint that the abuser was misusing it: "*He told me that*

he did not have the access to the Ring on his phone [...] so I didn't think he was watching us" (VS2). Similarly, some abusers lie about their *intent* when purchasing the device. For example, A14 had a case involving a suite of cameras around the house; the abuser "*claimed it was for their safety, so that he was protecting their family*" (A14). If IoT devices surfaced more information about who has accessed the device and what actions they took, victim-survivors could invalidate these false claims (Section 7).

5.2 Finding Hidden Devices

Abusers sometimes hide IoT devices such as spy cameras, GPS trackers, or AirTags to surveil victim-survivors. In these cases, the main challenge is finding those hidden devices.

Some participants asserted that when victim-survivors attempted to find hidden devices themselves, they used only "*physical inspection*" (A6). This included visually scanning the home for out-of-place devices, using a flashlight to reveal a hidden camera lens, or looking inside a car for something out-of-the-ordinary. A6 recalls: "*They'll start looking around their car until they find something that's either, it's a very clear AirTag or something else that's like, not a part of the car's machinery.*"

Victim-survivors also reached out to others for help finding hidden devices, according to most participants. A few asked for help from friends and family; for example, one victim-survivor found one hidden camera by accident, then enlisted a friend to look for more. Victim-survivors also contacted outside services like law enforcement, mechanics, and technicians to help them find devices. In one case, the victim-survivor "*took her car into the auto shop [...] and asked them to look for a tracking device on the car, and they found one*" (A3). In other cases, a Wifi technician also helped one victim-survivor find hidden cameras in their home, and law enforcement helped several victim-survivors find tracking devices on their vehicles or hidden cameras in their homes.

Though some victim-survivors were successful in finding hidden devices, others were never able to find anything. Our participants brought up four barriers that made it difficult to find hidden devices.

B3: Devices are designed to be discreet. Some participants brought up that many IoT devices, particularly item finders and GPS trackers, are easy to hide but difficult to find. A few advocates specifically pointed out that when these devices are placed in cars, they could be virtually impossible to find: "*You can kind of, like, put your hand in the engine and hide things pretty easily. [...] If you could squeeze your hand into and under a pipe, you're never gonna find that*" (A4).

In addition, IoT devices typically do not advertise their position after being placed; i.e., even if a device is not *meant* to be hidden, it is often still *able* to be hidden. The only devices which advertised their presence were AirTags, via Apple's anti-stalking features [12]; however, these features are not available to everyone, particularly since "*A lot of our clients also just don't have iPhones*" (A4).

B4: Manual inspection is the only way. In some interviews, participants said that victim-survivors had only ever used manual searching to find hidden devices. This worked for some victim-survivors, but not others; given the small size and hide-ability of many IoT devices, manual inspection is not always feasible. For example, when asked if they knew of any clients who had been able to find hidden devices themselves, A1 recalled, "*Honestly, I don't. I don't even know where I would look.*" Though detection tools exist (e.g., [11,70]), they were not helpful to these victim-survivors.

B5: Lack of relevant expertise. Some also mentioned that a lack of technology expertise makes it difficult to find hidden devices. Victim-survivors may not know "*what to look for and what to do*" (A1); when the only way to find hidden devices is through manual search, this uncertainty can prevent the search from even starting. Further, when victim-survivors suspected that a tracking device was placed in their car, it was difficult to search effectively without *car* expertise. In particular, it was difficult to identify when something was simply part of the car and when something was a tracking device. A4 recalled, "*One client had us look at something, and she was like, 'Is this part of my car or is this a tracker?' [...] I don't know anything about cars to know if it was.*"

B6: Outside services may not be able to help. About half of the participants said that when victim-survivors ask services like mechanics to help them find devices, those services may not be able to find anything, even if "*they had really tried, like they lifted the car up and searched the underside of it and everything*" (A5). Unfortunately, an unsuccessful search does not give victim-survivors peace of mind:

> *A lot of times, they won't find anything, and then the client doesn't always feel like, "Oh, good, everything's good now, they didn't find anything." Like they still feel like there is—that they are being watched. They just, it wasn't in that way, or the person missed it or something. (A3)*

Thus, not only is it difficult to identify IoT abuse, it is also difficult to *rule out* IoT abuse. In cases like A3 mentions, it's possible that there are no hidden devices present after all. But without rigorous measures to identify IoT abuse, victim-survivors in such scenarios may never get peace of mind.

5.3 Accidentally Identifying Abuse

In about half of the interviews, participants mentioned cases where victim-survivors identified abuse or found hidden devices by accident. Sometimes, known devices indicated abuse without prompting. For example, VS2 recalled seeing the abuser's contacts displayed on their smart speaker, a digital clue that his account was connected to the speaker. In another case, while the Wi-Fi technician was examining the router, the technician saw that there were hidden cameras connected to the router. Other times, hidden devices advertised their

presence purposefully (using Apple's stalking notifications) or inadvertently (by showing a low-battery light or falling out of position). In the future, these clues could be harnessed to intentionally indicate abusive behavior.

6 Mitigating IoT Abuse

After identifying IoT abuse, victim-survivors may choose to mitigate the abuse by making changes to their IoT devices, asking for help, or taking legal actions. Advocates, in turn, try to help victim-survivors by providing advice or directing them to other services. Despite a seemingly broad number of options, each one comes with hurdles that can prevent victim-survivors from mitigating the abuse. Fig. 6 summarizes these different strategies for mitigation and the associated barriers (B7–B21) we identify.

Importantly, because of the barriers we discussed in Section 5, many victim-survivors never find any proof that their partner is misusing IoT devices. While victim-survivors in this situation can still attempt to mitigate the abuse, they face additional barriers as a result.

B7: IoT abuse is not isolated. A barrier that reaches across all mitigations is the fact that IoT abuse is not an isolated issue. As some participants brought up, victim-survivors are often dealing with many forms of IPV concurrently. As a result, they may be trying to mitigate IoT abuse while experiencing multiple forms of trauma, going through a divorce, dealing with custody battles, seeking a restraining order, or moving, to name just a few scenarios. With so much going on, even seemingly simple mitigations to IoT abuse can be deprioritized or made more difficult:

> *They're trying to juggle personal safety and work and leaving a relationship and all these other things. And then I'm asking them to learn how to connect a router on top of it. (A6)*

> *If it were just the lights, I'm sure she would have less barriers. That would have just been like, switching the Wi-Fi or like kicking [the abuser] off. [...] But there's always more going on. (A4)*

This frustrating reality can prevent victim-survivors from attempting the mitigations we discuss in this section.

6.1 Device-Based Action

When abusers use IoT devices in abusive ways, an instinctive solution is to make changes to those devices to try and stop the abuse. Indeed, victim-survivors try many device-based actions in response to IoT abuse.

Physical changes. Most participants recalled victim-survivors who disabled the misused IoT device by resetting it, unplugging it, destroying it, or otherwise getting rid of it. This was a common choice for victim-survivors who found hidden tracking devices or cameras and wanted the surveillance to stop immediately; "*Most of them just want to remove it and take the battery out*" (A5). Similarly, multiple victim-survivors were convinced there was a tracking device in their cars, but never found one. To address the problem, A7 says, "*We've had a couple of those clients just get rid of the car, because they can't figure it out.*"

A more subtle option is to move the device to a different location, which was a technique noted by a few participants. When one client found an AirTag, for example, A8 recommended that the client "*should keep it, but maybe in a place that she's not carrying it around.*" Moving the device, rather than disabling it, reduces the device's capabilities somewhat without alerting the abuser that the abuse has been detected. It also allows the victim-survivor to keep evidence of the abuse on hand, which can be helpful later.

Configuration changes. Victim-survivors also try to reduce the abuser's access to the device or the associated account, according to a few participants. To revoke access entirely, victim-survivors change the password to the account or remove the abuser as a shared user. When accounts still need to be shared, victim-survivors may instead update the account to use their name and email address instead of the abuser's, which allows more control over the account information and billing. VS2 took both of these routes by removing their partner from the Amazon Household and separately "*changing the Roku account to be underneath my name*." Sometimes, these types of changes require the victim-survivor to contact the device manufacturer in order to initiate the change. For example, VS2 "*tried to call Amazon and I tried to call Ring in order to separate [the Ring doorbell] from his accounts*."

Victim-survivors also change non-access control configurations as a mitigation, according to some. They may change the Wi-Fi password, like VS2 did with help from a friend: "*He volunteered to change the Wi-Fi router password and all the connected devices because it's just a big jump.*" Others reduced the device's functionality by turning off notifications or removing batteries temporarily. VS1 recalled, "*When I left [...] I turned off the notifications*" on the home alarm system, which made it more difficult for their partner to notice when they escaped from the home.

Though there are several physical and configuration changes to choose from, making these changes is not always an option for victim-survivors.

B8: The abuser could notice changes. As noted by about half of the participants, a prohibitive barrier to device-based action is that the abuser might know about the changes. They may receive digital notifications of changes, either explicit (e.g., receiving an email) or implicit (e.g., no longer seeing the location of their tracking device, or the feed of their hidden camera). If the abuser is present in the home, they are also likely to notice physical changes such as a device that is in a different spot, is behaving differently, is off, or has been removed; as A5 describes, making these changes "*would be patently obvious. He would definitely know that you did that.*"

Stage	Goal	Barriers	Potential Solutions
Identifying IoT Abuse	Identify abuse via known devices	B1: IoT devices do not indicate abuse	Increased transparency
		B2: IoT devices are not seen a threat	Raising awareness
	Find hidden devices	B3: Devices are designed to be discreet	Increased transparency
		B4: Manual inspection is the only way	Tailored tools & services
		B5: Lack of relevant expertise	Tailored tools & services
		B6: Outside services may not be able to help	Training advocates, Tailored tools & services
Mitigating IoT Abuse	Any mitigation goal	B7: IoT abuse is not isolated	Training advocates, Tailored tools & services
	Make changes to IoT devices	B8: The abuser could notice changes	Abuse-aware design, Raising awareness
		B9: Victim-survivors don't know how to make changes	Abuse-aware design, Raising awareness
		B10: Devices are hard to get rid of	Raising awareness
		B11: Configuration changes are inconvenient	Abuse-aware design
		B12: Changes may be illegal or prohibited	Legal collaborations
	Get help from outside services	B13: Results are not guaranteed	Training advocates, Tailored tools & services
		B14: Outside services are not IoT abuse experts	Training advocates, Tailored tools & services
		B15: Seeking help is not always an option	Raising awareness
		B16: Advocates do not know where to send clients	Training advocates, Tailored tools & services
	Provide actionable advice for clients	B17: Advocates are not IoT abuse experts	Training advocates
		B18: Advocates have limited time	Training advocates, Tailored tools & services
		B19: Advocates have limited knowledge of each case	Tailored tools & services
	Seek legal action	B20: IoT abuse is not always perceived as illegal	Legal collaborations
		B21: Legal protections fail to consider IoT devices	Legal collaborations

Figure 6: Summary of our major findings. We describe the goals of victim-survivors and advocates when identifying or mitigating IoT abuse, the barriers they face when working towards these goals, and our proposed solutions.

If abusers notice these changes, the consequences can be dire. An abuser may confront the victim-survivor about a missing tracking device or attempt to place a new one. In one case, for example, law enforcement helped a victim-survivor remove a GPS tracker from her vehicle. However, the abuser knew where she worked and what her car looked like, meaning that "*days later, there would be a new one and she ended up with I think over 10 trackers over various months.*" (A14). If the abuser and victim-survivor live together, the abuser could also reverse any changes the victim-survivor makes. This is one reason VS2 did not get rid of their devices: "*Even if I got rid of them, he just would've went and bought new ones.*"

Finally, if the abuser notices changes, they may retaliate and the abuse could escalate. Facing such dangerous repercussions, many victim-survivors choose not to make any changes, even if that means living with surveillance:

> *Depending on the situation, [... it's] watching what you say and do in certain times, which sucks. But in some cases, it's life or death and that's what you have to do. (A1)*

B9: Victim-survivors don't know how to make changes. Some participants mentioned that victim-survivors do not always know what changes to make or how to make them. For example, one victim-survivor "*didn't know how to kick him out when he connected to the TV. It was kind of just waiting for him to get bored and move on to doing something else*" (A4). This is a point of frustration for tech-savvy victim-survivors as well as non-tech-savvy victim-survivors; VS2 is "*fairly comfortable*" with technology, but still ran into issues when trying to reset smart light bulbs ("*The smart bulbs, I don't see anything on them to press*").

To help figure out what to do, victim-survivors sometimes search online for documentation or other informational resources. However, the information they see may already be out of date. When VS2 used online advice to made configuration changes to their smart speaker, "*it wasn't exactly labeled the correct subcategories as when that advice was given out online, probably due to an update*." Further, the complex design of IoT devices means that mitigations are also complex. For example, devices can have more than one access point, such as an Alexa account and an Amazon Household. To revoke an abuser's access, victim-survivors need to know about and address each of these access points.

B10: Devices are hard to get rid of. Disabling, destroying, and removing devices is one popular mitigation method. However, as a few participants noted, many of these devices are necessary for the victim-survivor's safety and comfort. For example, when one victim-survivor considered removing misused smart lights, "*it was still difficult to figure out how to keep some light so that she could feel comfortable and sleep okay*" (A4). If the victim-survivor does get rid of devices, it can also be expensive. VS2 believed that if they got rid of the home security system, their partner would just purchase a

new one; as a result, "*it would put us in more of a financial bind at that point, too. So it's kind of like a catch-22*" (VS2). Getting rid of IoT devices may mitigate the IoT abuse, but it may also introduce new problems.

B11: Configuration changes are inconvenient. Changing passwords to accounts, changing the Wi-Fi password, and making other kinds of configuration changes is cumbersome, according to a few participants. VS2 recounts that when a friend came by to reset the Wi-Fi password and reconnect all of the IoT devices, "*it took him a couple hours just because of the bulk of it.*" Victim-survivors may also be wary of losing data when reconfiguring or resetting devices; for one of A6's clients, "*there were some devices she wasn't willing to [reset]. She had information on there that she wanted to retain.*"

B12: Changes may be illegal or prohibited. Finally, some participants explained how victim-survivors can be blocked from taking device-based action because of laws or the device manufacturer's policies. First, victim-survivors may face legal issues if the device (or account) is owned by the abuser or is *marital property* (legally owned by both parties in the marriage). VS2 describes that when trying to put their smart light bulbs under their name, they were told "*it was something that would have to be settled in court*" as part of their ongoing divorce. This was particularly frustrating given that the couple was separated, with VS2 living in the previously-shared home with their children and smart home devices:

> *There should be more thought into how to claim, okay, [the devices are] in my house, they're on my property, they're mine. It should not be something disputed. (VS2)*

Besides property issues, victim-survivors can be blocked by manufacturers when trying to take action. For example, during their separation, VS2 also wanted to remove their partner from the previously-shared Ring doorbell. VS2's Amazon account was connected to all of the smart home devices, but it was the *partner*'s Ring account connected to the doorbell; when VS2 called Amazon to sort it out, "*they told me I could not unlink it unless I had his password for his Ring account.*" (VS2).

Finally, there are some device-based mitigations for IoT abuse which are prohibited. For Bluetooth devices, A5 says, "*the only way that you can really stop it is by using like a Bluetooth jammer. But that's, you know, illegal.*"

6.2 Getting Outside Help

When they cannot take device-based action, victim-survivors often turn to outside services for help. In some interviews, we learned how victim-survivors independently sought help from hotlines, law enforcement, and mechanics when trying to mitigate the abuse. Additionally, in most interviews, advocates explained how they direct victim-survivors to outside services—usually, because they felt the victim-survivor would get better help from these other services.

Victim-survivors and advocates looked to multiple types of outside services, tailored to different concerns:

- *IPV experts*: VSPs, tech abuse services like CETA [2];
- *Tech experts*: device manufacturers, technology retailers (e.g., Best Buy), mechanics, car dealers;
- *Legal/government services*: police, judges, attorneys;
- *Online tools and resources*: informational websites like techsafety.org [5], online tools and apps like Fing [3].

These outside services have helped clients in the past not only by identifying abuse, as discussed, but also by removing tracking devices or helping victim-survivors take back control of devices. For example, one abuser hijacked a smart thermostat; then, in a restraining order hearing, "*the judge was like 'What is the code?' And then the client who was living in the house was able to reset the code*" (A1).

Occasionally, outside services can offer relief to victim-survivors by taking a burden off their shoulders. Unfortunately, this is not always what happens.

B13: Results are not guaranteed. The most pressing issue, according to some, is that outside services cannot guarantee results for a victim-survivor. For one thing, the helpfulness of outside services can greatly depend on the specific person who is helping. A1 has seen this with the police; while sometimes police officers are helpful, "*other times, I feel like they'll just take their report and like, 'We'll follow up with you'*" (A1).

Regardless of the person helping, outside services may simply not succeed in helping a victim-survivor find evidence of abuse, secure a restraining order, or remove a tracking device from their car. "*It just kind of depends. Which is also scary as a person trying to report some things, because you don't know what's gonna happen to you*" (A1). Without knowing if outside services will be worth their time, victim-survivors are less likely to go through the effort of seeking help.

B14: Outside services are not IoT abuse experts. One particular reason that outside services can be unhelpful is that these services are not experts in IPV, technology, or IoT abuse as a whole. A few participants noted that this lack of expertise makes it more difficult for outside services to help victim-survivors. For example, tech service providers are not trained to provide trauma-informed care, since that is not the purpose of their services. Some services lack expertise in both trauma-informed care *and* technology; for example, when VS2 asked a police officer for help handling IoT abuse, the officer replied, "*You probably know more about this than I do.*"

B15: Seeking outside help is not always an option. A few participants also brought up that victim-survivors facing IoT abuse may simultaneously be coping with other forms of abuse or stressors, which can make it more difficult to seek outside help. For example, if the victim-survivor is struggling financially—perhaps due to financial abuse—they may not be able to afford the cost of outside services. Additionally, victim-survivors of IoT abuse or other forms of tech abuse can be fearful of technology. For this reason, one of A6's clients

stopped calling the VSP due to "*concerns about the security of our systems.*"

Victim-survivors may also have too much going on to prioritize going to an outside service for help with the IoT abuse. A8 recalls that for one victim-survivor, "*There was so much going on. [...] It was too much for her to just like have to make an appointment for someone to search her car.*"

B16: Advocates do not know where to send clients. One avenue for victim-survivors to get outside help is when advocates direct them to other services. This was one of the most common techniques advocates used for helping victim-survivors with IoT abuse situations (often because advocates did not feel equipped to help with IoT abuse themselves). However, some advocates said they were not always aware of what services would be helpful to clients. A1 explains, "*I kind of don't know where to steer them.*" This may be due to limited training on IoT abuse and tech abuse generally, as we will discuss in Section 6.3; it may also be simply because there are no services dedicated for IoT abuse.

6.3 Providing Actionable Advice to Clients

Besides directing victim-survivors to outside services, advocates most often helped victim-survivors by providing advice. In most cases, they performed established advocate support tasks like helping the victim-survivor safety plan, providing financial support if possible, and giving generic advice (e.g., "*Oh, can you change passwords?*" (A1)).

A few advocates also worked to provide specific advice for the IoT abuse their clients were experiencing. Often, this meant doing some research on the technical aspects of the case (e.g., how to use or reconfigure the specific devices involved in the case) and sometimes the legal aspects of the case (e.g., whether a specific type of IoT abuse is illegal). Then, the advocates provided specific advice on how clients could mitigate abuse by sharing online resources, teaching clients about the information they learned, and guiding them through some potential mitigation steps.

When advocates are unsure what to do, they lean on the people around them, according to some advocates. For example, though A16 feels that handling smart devices is "*not in my tool bag*," they also felt strongly that they could get help from other advocates at the VSP:

> *Somebody has went through this, somebody has helped [someone] with this, you know, so in a way I don't feel limited. [...] I feel comfortable to just say, "Hey, just give me one moment. I'm gonna get somebody that can better serve you." (A16)*

Though these strategies work for many advocates, three barriers make it more difficult to provide actionable advice.

B17: Advocates are not IoT abuse experts. The first barrier all of the advocates face is a lack of knowledge of IoT abuse or of tech generally. Advocates are not always tech savvy and/or have not received the proper training to be able to help with tech abuse. This means that they may not know the answer to IoT abuse, or where to look for answers. A8 shared, "*Since I'm not smart device savvy, sometimes I'm kind of unsure about, you know, answers or strategies, or what to do, or resources.*" Thus, sometimes, advocates can only "*reiterate what I saw on Google*" (A4). Even tech-focused advocates do not always know how to deal with IoT abuse situations; though A9 has a strong technology background and is a tech abuse advocate, they shared, "*I don't feel as if I'm an expert on it. I don't use or [am] not familiar with many devices.*"

Part of the problem is that IoT devices vary greatly and span lots of domains (appliances, security systems, tracking devices, etc.), meaning that it's difficult to be an expert in how to use all types of devices. Additionally, "*everything is changing so often,*" says A7. "*We're never going to know it all and we're never gonna be able to catch it all.*" These factors are exacerbated by the fact that advocates have had little experience handling IoT abuse, since it is a newer phenomenon than other kinds of tech abuse.

B18: Advocates have limited time. Advocates work with a large volume of clients at one time, giving them little time to spend with each client. According to some, this means that if advocates do not immediately know how to mitigate IoT abuse, they may not have time to do the research required to give a client advice on a situation. A2 notes "*I don't know that the level of research we have the capacity to do would necessitate particular specialized resources, because I don't know that we'd have the time to go that far and search.*"

Advocates also sometimes help clients on demand, or over a single phone call, and thus have to try to give advice right away without time to prepare. In these situations, advocates do not have the luxury to say "*Oh, let me go to this webinar, let me go through this training*" (A8).

In addition, some mentioned that VSPs as a whole do not have the resources or time to help every victim-survivor who comes to them. If a victim-survivor is not able to find proof of the IoT abuse—a problem many face, as we've discussed—the VSP may not have the resources to help them. VS1 experienced this when trying to escape a surveillant household:

> *I didn't really have any proof of anything. [...] Going to file any paperwork, unless you're bleeding or show visible bruises somewhere, they don't care. (VS1)*

B19: Advocates have limited knowledge of each case. Finally, advocates often see clients for a short time, meaning they cannot learn every detail of potentially years-long abuse. "*We get thrown into people when it's random,*" A1 describes. "*So it's like, this has been going on for years and we're just here now. We obviously don't know every detail of everything, and we just go off of what we know or feel out is happening.*"

To make things more complex, victim-survivors may have a hard time describing the IoT abuse they are experiencing. Advocates can only work from this information, which may not be entirely correct or easy to understand. These factors make it difficult to give advice because, as some advocates

pointed out, there is no universal solution to IoT abuse; the most effective mitigation for IoT abuse greatly depends on the details of each situation.

After helping someone with an IoT abuse case, advocates often do not know the outcome. They commonly offer advice over a phone call or in a single meeting, then never hear from the client again or learn how the case went. A9 describes, "*You actually don't know, did this work? Did they feel comfortable?*" If advocates do not learn whether their advice was helpful, they cannot adjust or improve their advice for future clients.

6.4 Legal Action

The final type of mitigation, mentioned by almost all participants, involves legal action. First, victim-survivors may seek protection from their abuser by seeking a restraining order. For example, after finding hidden cameras, one victim-survivor "*filed a restraining order and removed [the abuser] from the premises*" (A8). As part of these legal measures, victim-survivors can also regain control of their devices. As previously mentioned, one abuser changed the code for the smart thermostat to lock the victim-survivor out entirely, but the victim-survivor was able to gain back control during the restraining order hearing.

Victim-survivors can also seek legal charges against the abuser for IoT abuse, some participants told us. For instance, IoT abuse can sometimes constitute a violation of a no-contact order. A10 had a case where the abuser was barred from accessing the family home, but he was accessing recording from the Alexa within the home as well as using the account to make deliveries to the home. Law enforcement asserted that "*he absolutely was not allowed to do any of that. He was charged with a gazillion more bail jumping counts*" (A10). Evidence of IoT abuse can also be added to a stalking case, bolstering an argument for an abusive pattern of behavior.

Legal action is an attractive option, particularly when other options are unavailable (e.g., when the abuser is present in the home). Unfortunately, about half of the participants described how legal action cannot always stop IoT abuse.

`B20`: IoT abuse is not always perceived as illegal. As discussed above, evidence of IoT abuse can provide evidence of stalking or other long-term criminal behavior. However, as about half of the participants noted, many forms of IoT abuse are not *by themselves* illegal. This is especially perceived to be true when an abuser is misusing IoT devices they own; for example, there is no law preventing someone from looking at the feed of their own Ring Doorbell, regardless of whether they are using it to surveil their partner. A1 described how these types of IoT abuse could potentially get a victim-survivor a restraining order; "*but is that a criminal charge? No, it is a civil action*" (A1).

`B21`: Legal protections fail to consider IoT devices. Similarly, a few participants described that if a victim-survivor *does* succeed in taking legal action for IoT abuse or other abuse they are experiencing, the associated legal protections may not address IoT abuse. For instance, if someone receives a restraining order, the abuser is required to leave the shared household, but they are not explicitly required to relinquish control over the digital household (the IoT devices within the home). VS2 experienced this firsthand:

> *It's extremely frustrating and unfair that somebody could be not physically there, but digitally there, watching your every move. And that's okay with the courts. [...] If I get a restraining order, why shouldn't that apply to smart devices? (VS2)*

7 Discussion

Our 20 interviews surfaced a number of real-world instances of IoT abuse, strategies that advocates and victim-survivors use to identify and mitigate IoT abuse, and barriers they face in doing so. These insights add depth to the community's understanding of IoT abuse and point to necessary solutions.

First, our participants described real-world examples of many of the varieties of IoT abuse hypothesized [38, 39, 46] or reported [40, 60, 61] in prior work. We saw that, similar to "dual-use" apps vs. spyware [15, 24], abusers take advantage both of devices meant for spying (like hidden cameras) as well as devices that have a separate, benign purpose (like Ring doorbells). By surfacing these stories, we help raise awareness of IoT abuse within the security community.

Second, we flesh out the barriers victim-survivors and advocates face when dealing with IoT abuse. In prior work, Tanczer et al. [61] reported that it is "really hard to roll [... an abuser's] access back" on IoT devices. Our findings echo this concern and elaborate that a device's opaque design, a victim-survivor's lack of technical expertise, a manufacturer's unwillingness to help, and a lack of legal recourse can all make it more difficult to revoke an abuser's access to an IoT device. Tanczer et al. also hinted that the "camouflaged" nature of IoT devices makes it more difficult to identify abuse; as we learned, this phenomenon includes both *hidden* devices which do not announce themselves, as well as *overt* devices which do not indicate abusive behavior. Because our findings concretize these barriers, they allow us to specify clear paths towards removing the barriers (Section 7.2).

7.1 IoT Abuse vs. Broader Tech Abuse

Zooming out, we highlight why IoT abuse is distinct from other forms of tech abuse in IPV. The barriers we identified support four main reasons why IoT abuse requires unique attention. First, many IoT devices are *designed* to control and monitor the physical environment, which enables heightened surveillance and harassment (`B1`, `B2`, `B9`, `B19`). Second, many IoT devices are designed to be *shared* among all users in a home, which, in IPV, may include an abusive partner (`B8`, `B10`, `B11`). Third, many IoT devices can be easily hidden by design, making it easier for abusers to surveil covertly and

harder for victim-survivors to find hidden devices (B3-B6). Finally, because of the novelty and technical complexity of IoT devices, advocates and victim-survivors are less familiar with these devices and how they can be misused (B5, B8, B13, B15, B16). These unique features of IoT abuse require tailored solutions, which we will discuss in Section 7.2.

Similarly, we provide evidence that many of the tensions and complexities of general tech abuse are still present in IoT abuse, but may have more dire consequences. For example, Freed et al. [30] pointed out that tech abuse can make a victim-survivor fearful of technology. With IoT abuse, we found that because there is no definitive way to *rule out* IoT abuse, that fear of technology extends to the victim-survivor's entire home, as well as their possessions. As another example, Freed et al. [30] described how the legal system is not built to address tech abuse. While some legal advances have been made to combat phone-based tech abuse—e.g., the Safe Connections Act of 2022 makes it easier for victim-survivors to separate from a shared phone plan with their abuser [9]—we show that for IoT abuse, a lack of involvement from the legal system is still very much a problem.

7.2 Towards Removing Barriers

Similar to other tech abuse in IPV [29, 42], addressing IoT abuse requires a multi-pronged solution with cooperation of different stakeholders. Fig. 6 summarizes potential solutions to overcoming the barriers we have described throughout this paper. Our proposed solutions echo those of Tanczer et al. [60] and Lopez-Niera et al. [40]; we draw on our findings to outline more concrete directions towards these solutions.

Increase the transparency of IoT devices. Most participants noted that identifying IoT abuse is challenging because (1) hidden devices are difficult to find and (2) known devices do not reveal abusive behavior. Manufacturers of IoT devices can help victim-survivors identify IoT abuse by increasing the transparency of their devices' presence and activities.

To address (1), manufacturers of small, hideable IoT devices should make their devices more conspicuous. Devices must announce their presence using sound, light, wireless packets, or other means. For example, a low-battery light revealed a hidden camera in one case; if the light flickered periodically, regardless of the battery life, the victim-survivor may have found the camera sooner. Towards this goal, Apple introduced a beeping sound to alert bystanders that an AirTag may be tracking their location [13]. Of course, these announcements must be carefully designed to preserve the devices' intended use case, such as theft prevention.

Towards (2), IoT devices should have detailed logs of user activities like viewing a camera feed, checking the security system status, or changing the temperature. Importantly, these logs should also contain information on who is doing these actions (e.g., "User A changed the temperature at [time]" or "User B viewed the location of device X at [time]"). Some devices have implemented logging already; for example, with a paid subscription, Ring Doorbells record the time when a user viewed the live camera feed [6]. However, Ring currently does not specify which user performed that action, and the log can be deleted by any user of that camera, negating the usefulness of the log in IPV scenarios. Therefore, these logs must also be protected from deletion or manipulation.

When designing these logs, researchers must carefully consider the potential drawbacks. For example, the same logs that provide transparency to a victim-survivor may at the same time provide another vector for surveillance. This is especially concerning given that we have identified real-world examples of abusers using activity logs maliciously (Section 4).

Redesign IoT devices with abuse in mind. Given the extent of harm IoT devices can cause to IPV victim-survivors, manufacturers should involve IPV advocates and victim-survivors and consider an adversarial intimate partner threat model [57] during design. Doing so could reveal any potential for misuse and allow manufacturers to proactively mitigate this misuse.

In particular, one way manufacturers could proactively mitigate misuse is by rethinking access control for shared devices. IoT devices are designed to be shared among household members, but in practice, they do not guarantee equal control or access to all residents. This hinders a victim-survivor's ability to take action. To alleviate this, manufacturers should adopt a new paradigm for device sharing. We propose (with caveats for children, guests, etc.) that if an IoT device can surveil or control a home, anyone living in that home should be able to control the device and anyone no longer living in that home should not. The security community should investigate this type of presence-based access control system (e.g., [68]) in the context of IPV. There will be challenges to implementing such a system—e.g., the legal definition of ownership may conflict with this new paradigm—but if successful, this would empower victim-survivors to take control over the devices in their home and prevent abusers from accessing devices after they no longer live in the house.

Train advocates and outside services. On the support system side, we need to foster greater awareness of IoT abuse among advocates, law enforcement, and other other service providers such as car mechanics and network technicians. Our participants lamented that these groups do not receive the right training to be able to properly help victim-survivors with IoT abuse. As a result, victim-survivors rarely receive effective help from these services.

To educate service providers about IoT abuse, we need to design training programs which raise awareness of the different types of IoT abuse. For advocates, this training should also provide resources they can reference and share with clients to help navigate, identify, and mitigate IoT abuse. For other services in the community such as mechanics, the training should prepare them to use their specific expertise to support victim-survivors. This type of training will strengthen the

networked care already ingrained in advocacy [56], allowing advocates to point to services and say confidently, "*Hey, these people can help you*" (A7).

Create tailored tools & services. Even with comprehensive training, existing services are limited because they are not designed for IoT abuse situations. We need to provide victim-survivors with tailored tools and resources they can leverage to combat IoT abuse. For example, though off-the-shelf apps [35, 51, 70], handheld tools [11], and academic systems [53, 54] exist for detecting hidden devices, victim-survivors did not reach for these methods. Clearly, these existing methods are not accessible to everyday users who need them. The security community urgently needs to design detection tools which are easy for victim-survivors to use.

In addition, the security community should create a database of advice for people experiencing IoT abuse as a one-stop-shop for online help. This could be a collaborative effort, kept up-to-date by a suite of volunteers. The Clinic to End Tech Abuse (CETA) [2] from Cornell Tech has already gotten a start to this by creating a list of collaborative guides for different types of tech abuse, including IoT abuse [4, 10].

Ideally, the burden to deal with IoT abuse could fall on an expert consultant rather than a victim-survivor. Thus, a more ambitious solution would be to create specialized services for IoT abuse mitigation. One way to create these services would be expanding existing tech abuse clinics like CETA to cover IoT abuse. Another option is to design entirely new services tailored to IoT abuse. For example, a few advocates requested a service that could visit a victim-survivor's home and "*get the scoop*" (A1) on their devices. Such a service may be too risky to offer, especially if the abuser also lives in the home, but we envision a future program (similar to [36]) or handheld "magic wand" device that has the same capabilities without jeopardizing safety. These services should be available to victim-survivors even if they do not want to involve law enforcement. Tailored resources like this could provide victim-survivors with a definitive, trustworthy place to turn—a way to finally get peace of mind.

Raise awareness of IoT abuse. A barrier that prevented victim-survivors from identifying IoT abuse was their mindset around smart devices: before experiencing abuse, victim-survivors are not aware of the risks of IoT devices or how they could be used for abuse. Had victim-survivors been given this information at the time of device purchase, they could have identified IoT abuse earlier, configured devices to prevent abuse, or avoided purchasing the devices at all. To raise awareness of the risks of IoT devices, two actions are needed. First, manufacturers should be required to advertise the risks of their devices on the package. This information could be integrated into the existing notion of privacy nutrition labels which display the privacy and security practices of the device [26]. Second, as requested by four advocates, youth education should teach children about IoT abuse and, more broadly, what healthy and unhealthy technology use looks like in relationships.

Collaborate with legal experts. Finally, technologists should collaborate with legal experts to create more legal options for victim-survivors. Consistent with prior work [30, 56], our participants described how the U.S. legal system has sometimes failed victim-survivors who are experiencing IoT abuse. To protect victim-survivors, we need to update laws and regulations to address IoT abuse. For example, manufacturers should have clear policies and active warnings against the use of their devices for spying or harassing other parties. Policymakers should also update legislation to define IoT devices and associated accounts as part of the home so that accessing them will be considered as accessing the home. This will ensure, for example, if someone is legally required to leave a home due to a restraining order, they should also be required to relinquish control of the IoT devices in the home.

8 Conclusion

As IoT devices become more popular, they are beginning to be (ab)used in intimate partner violence. This IoT abuse has been reported in news stories and hypothesized in preliminary studies, but the details of this type of abuse remain elusive. We address this gap by performing the first interview study focused on IoT abuse. By interviewing 17 advocates and 3 victim-survivors with knowledge of real-world IoT abuse, we surface details about the types of abuse that are occurring, strategies victim-survivors use to identify and mitigate IoT abuse, and 21 specific barriers that victim-survivors and advocates face during this process. For example, the design of IoT devices and a lack of available resources leaves victim-survivors without proof of the IoT abuse they are experiencing. Our findings add much-needed depth to our understanding of IoT abuse and point towards solutions which can help victim-survivors in the future, such as more transparent designs for IoT devices and improved awareness of IoT abuse among advocates, community services, and the general public.

Acknowledgments

We are deeply grateful to the victim-survivors and advocates who participated in our study, as well as the community members who helped us refine the study. We also thank the anonymous reviewers and the shepherd for their insightful feedback. This research was partly funded by University of Wisconsin—Madison Office of the Vice Chancellor for Research and Graduate Education with funding from the Wisconsin Alumni Research Foundation.

References

[1] AirTag. Apple, https://www.apple.com/airtag/. 1, 2, 3

[2] Clinic to end tech abuse. Clinic to End Tech Abuse, https://www.ceta.tech.cornell.edu/. 11, 15

[3] Fing | Network and IP scanner for WiFi security. Fing, https://www.fing.com/. 11

[4] Resources. Clinic to End Tech Abuse, https://www.ceta.tech.cornell.edu/resources. 15

[5] Safety net project. National Network to End Domestic Violence (NNEDV), https://techsafety.org. 11

[6] Video recordings. Ring, https://support.ring.com/hc/en-us/articles/360030587812-Video-Recordings. 14

[7] Devastatingly pervasive: 1 in 3 women globally experience violence. World Health Organization Joint News Release, https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence, March 2021. 2

[8] Intimate partner violence. National Institute of Justice, https://nij.ojp.gov/topics/crimes/violent-crimes/intimate-partner-violence, September 2021. 2

[9] Bills signed: H.R. 7132 and S. 4524. The White House, https://www.whitehouse.gov/briefing-room/legislation/2022/12/07/bills-signed-h-r-7132-and-s-4524/, December 2022. 14

[10] General IoT and smart home devices security tips. Clinic to End Tech Abuse, https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_11dec6cea7554684b50b56f73ec8a985.pdf, June 2022. 15

[11] JMDHKK Anti Spy RF Detector Wireless Bug Detector Signal for Hidden Camera Laser Lens GSM Listening Device Finder Radar Radio Scanner Wireless Signal Alarm. Amazon, https://www.amazon.com/Detector-Wireless-Signal-Listening-Scanner/dp/B07B93347H/ref=sr_1_4, 2022. 8, 15

[12] An update on AirTag and unwanted tracking. Apple statement, https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/, February 2022. 8

[13] What to do if you get an alert that an AirTag, find my network accessory, or set of AirPods is with you. Apple, https://support.apple.com/en-us/HT212227, 2022. 14

[14] Otter.ai – Voice meeting notes & real-time transcription. https://otter.ai, 2023. 4

[15] Majed Almansoori, Andrea Gallardo, Julio Poveda, Adil Ahmed, and Rahul Chatterjee. A global survey of Android dual-use applications used in intimate partner surveillance. *Proceedings on Privacy Enhancing Technologies*, 1:20, 2022. 2, 3, 13

[16] Shaowen Bardzell and Jeffrey Bardzell. Towards a feminist HCI methodology: social science, feminism, and HCI. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 675–684, 2011. 5

[17] KELLY Bartholow, BOBBY Milstein, M Kathleen, E McLellan-Lemal, and KM MacQueen. Team-based codebook development: Structure, process, and agreement. *Handbook for team-based qualitative research. Lanham, MD: Rowman AltaMira*, pages 119–35, 2008. 4

[18] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. Ethical practices for security research with at-risk populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 546–553. IEEE, 2022. 3, 4, 5

[19] Brian Bourke. Positionality: Reflecting on the research process. *The qualitative report*, 19(33):1–9, 2014. 5

[20] Nellie Bowles. Thermostats, locks and lights: Digital tools of domestic abuse. The New York Times, https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html, Jun 2018. 1, 3

[21] Kaitlin M Boyle and Kimberly B Rogers. Beyond the rape "victim"–"survivor" binary: How race, gender, and identity processes interact to shape distress. In *Sociological Forum*, volume 35, pages 323–345. Wiley Online Library, 2020. 2

[22] Albert Fox Cahn. Apple's AirTags are a gift to stalkers. Wired, https://www.wired.com/story/opinion-apples-air-tags-are-a-gift-to-stalkers/, May 2021. 1, 3

[23] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky spy devices and defective detectors: The ecosystem of intimate partner surveillance with hidden devices. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2023. 3

[24] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018. 2, 3, 13

[25] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. Domestic violence and information communication technologies. *Interact. Comput.*, 23(5):413–421, September 2011. URL: http://dx.doi.org/10.1016/j.intcom.2011.04.006. 2

[26] Pardis Emami-Naeini. Privacy and security nutrition labels to inform IoT consumers. In *USENIX Enigma*, 2021. 15

[27] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019. 5

[28] 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):1–24, 2019. 2

[29] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise" How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–13, 2018. 2, 5, 14

[30] 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):1–22, 2017. 2, 4, 5, 14, 15

[31] Christine Geeng and Franziska Roesner. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019. 3

[32] Makda Ghebreslassie. 'Stalked within your own home': Woman says abusive ex used smart home technology against her. CBC News, https://www.cbc.ca/news/science/tech-abuse-domestic-abuse-technology-marketplace-1.4864443, November 2018. 1, 3

[33] Bridget A Harris and Delanie Woodlock. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, 59(3):530–550, 2019. 2

[34] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 105–122, 2019. 2, 4

[35] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. AirGuard - protecting Android users from stalking attacks by Apple Find My devices. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '22, page 26–38, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3507657.3528546. 15

[36] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. IoT Inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(2):1–21, 2020. 15

[37] Roxanne Leitão. Digital technologies and their role in intimate partner violence. In *Extended abstracts of the 2018 CHI conference on human factors in computing systems*, pages 1–6, 2018. 2

[38] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, pages 527–539, 2019. 1, 2, 3, 5, 13

[39] Karen Levy and Bruce Schneier. Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1), 2020. 2, 3, 5, 13

[40] 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. 3, 5, 13, 14

[41] Ryan Mac and Kashmir Hill. Are Apple AirTags being used to track people and steal cars? New York Times, https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html, December 2021. 1, 3

[42] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2189–2201, 2017. 2, 14

[43] Phoebe Moh, Pubali Datta, Noel Warford, Adam Bates, Nathan Malkin, and Michelle L Mazurek. Characterizing everyday misuse of smart home devices. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 1558–1572. IEEE Computer Society, May 2023. 3

[44] Anna Moore. 'I didn't want it anywhere near me': how the Apple AirTag became a gift to stalkers. The Guardian, https://www.theguardian.com/technology/2022/sep/05/i-didnt-want-it-anywhere-near-me-how-the-apple-airtag-became-a-gift-to-stalkers, September 2022. 1

[45] Emily Namey, Greg Guest, Lucy Thairu, and Laura Johnson. Data reduction techniques for large qualitative data sets. *Handbook for team-based qualitative research*, 2(1):137–161, 2008. 4

[46] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In *Proceedings of the new security paradigms workshop*, pages 1–15, 2019. 2, 3, 5, 13

[47] Eva PenzeyMoog. *Design for safety*. A Book Apart, 2021. 2, 5

[48] Eva PenzeyMoog and Danielle C Slakoff. As technology evolves, so does domestic violence: Modern-day tech abuse and possible solutions. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited, 2021. 5

[49] K Andrew R Richards and Michael A Hemphill. A practical guide to collaborative qualitative data analysis. *Journal of Teaching in Physical Education*, 37(2):225–231, 2018. 5

[50] Kevin A 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 *2020 IEEE Symposium on Security and Privacy (SP)*, pages 626–643. IEEE, 2020. 2

[51] Royal Tech App Studio. Detect bug - camera microphone. Google Play Store, https://play.google.com/store/apps/details?id=com.royaltechapps.hiddencameradetector&hl=en_US&gl=US, 2022. 15

[52] Johnny Saldaña. The coding manual for qualitative researchers. *The coding manual for qualitative researchers*, pages 1–440, 2021. 4

[53] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. Lumos: Identifying and localizing diverse hidden IoT devices in an unfamiliar environment. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, August 2022. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/sharma-rahul. 15

[54] Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava. I always feel like somebody's sensing me! A framework to detect, identify, and localize clandestine wireless sensors. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1829–1846, 2021. 15

[55] Julia Slupska. Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review*, 15(1):83–100, 2019. 3

[56] Julia Slupska and Angelika Strohmayer. Networks of care: Tech abuse advocates' digital security practices. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 341–358, 2022. 2, 5, 15

[57] Julia Slupska and Leonie Maria Tanczer. Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited, 2021. 3, 14

[58] Sharon G. Smith, Xinjian Zhang, Kathleen C. Basile, Melissa T. Merrick, Jing Wang, Marcie jo Kresnow, and Jieru Chen. The national intimate partner and sexual violence survey (NISVS): 2015 data brief – updated release. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, https://www.cdc.gov/violenceprevention/pdf/2015data-brief508.pdf, 2018. 2

[59] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. Abuse vectors: A framework for conceptualizing IoT-enabled interpersonal abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2023. 3

[60] Leonie Tanczer, Isabel Lopez-Neira, Simon Parkin, Trupti Patel, and George Danezis. Gender and IoT research report: The rise of the Internet of Things and implications for technology-facilitated abuse. https://discovery.ucl.ac.uk/id/eprint/10140276/1/giot-report.pdf, 2018. 3, 5, 13, 14

[61] Leonie Maria Tanczer, Isabel López-Neira, and Simon Parkin. "I feel like we're really behind the game": Perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of gender-based violence*, 5(3):431–450, 2021. 1, 2, 3, 5, 13

[62] 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 *29th USENIX Security Symposium (USENIX Security 20)*, pages 1893–1909, 2020. 2

[63] 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. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021. 2

[64] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care infrastructures for digital security in intimate partner violence. In *CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2022. 2, 5

[65] Bessel Van der Kolk. The body keeps the score: Brain, mind, and body in the healing of trauma. *New York*, 2014. 3

[66] Delanie Woodlock. The abuse of technology in domestic violence and stalking. *Violence against women*, 23(5):584–602, 2017. 2, 5

[67] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017. 7

[68] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 159–176, 2019. 14

[69] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–20, 2018. 7

[70] Zeehik IT Zon. Hidden devices detector. Google Play Store, https://play.google.com/store/apps/details?id=com.zeehikitzon.hiddendevicesdetector&hl=en_US&gl=US, 2022. 8, 15

[71] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. The role of computer security customer support in helping survivors of intimate partner violence. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 429–446, 2021. 2