Networks of Care: Tech Abuse Advocates' Digital Security Practices

Julia Slupska
University of Oxford

Angelika Strohmayer
Northumbria University

Abstract

As technology becomes an enabler of relationship abuse and coercive control, advocates who support survivors develop digital security practices to counter this. Existing research on technology-related abuse has primarily focused on describing the dynamics of abuse and developing solutions for this problem; we extend this literature by focusing on the security practices of advocates working "on the ground", i.e. in domestic violence shelters and other support services. We present findings from 26 semi-structured interviews and a data walkthrough workshop in which advocates described how they support survivors. We identified a variety of intertwined emotional and technical support practices, including establishing trust, safety planning, empowerment, demystification, supporting evidence collection and making referrals. By building relationships with other services and stakeholders, advocates also develop networks of care throughout society to create more supportive environments for survivors. Using critical and feminist theories, we see advocates as sources of crucial technical expertise to reduce this kind of violence in the future. Security and privacy researchers can build on and develop these networks of care by employing participatory methods and expanding threat modelling to account for interpersonal harms like coercive control and structural forms of discrimination such as misogyny and racism.

1 Introduction

Technologies and digital systems are being incorporated into existing patterns of abuse to harm intimate partners and strangers alike. Sometimes these technologies are built specifically for this purpose (e.g. the case of "stalkerware" apps [12]), but more often perpetrators of this violence use mundane, everyday technologies to control, coerce, or harm their victims [26]. Advocates and support organisations have developed strategies that counter this abuse and support survivors in developing digital safety practices.

Security researchers have started to discuss technology-enabled abuse in intimate relationships (often shortened to 'tech abuse') and other forms of coercive control [12, 34, 44, 75]. For example, many researchers (both within and outside of security studies) have (1) built an understanding the dynamics of tech abuse and (2) developed solutions that aim to reduce this kind of violence. Both of these kinds of work often jump to conclusions about what security researchers, developers, or designers can do to tackle this issue. However, it is seldom that we examine what is already going on outside our field to learn from the expertise of those who have been doing this work for a long time. With this paper, we counter this tendency and instead bring lenses of care and empowerment into security discourse based on the security work of advocates who support victim-survivors[1] of tech abuse.

To carry out our analysis, we first need to understand the boundaries of what security research can and cannot do, and extend the frame of reference we have about violence and technologies within the security community. We draw on two areas of security research: (1) critical security studies and (2) feminist security studies. Both these areas focus on the power dynamics inherent in security practices. Critical security studies draw on disciplines like sociology and anthropology to question the underlying logic of security, arguing security is often used as a justification for imposing control in a way that can limit peoples' rights or freedoms and lead to authoritarianism [15, 50, 58, 61]. Feminist security studies on the other hand shifts our focus away from technical systems, hackers, or the military, and asks us to think at the level of interpersonal security and how social relationships can be sources of both security and insecurity [40].

Using these two frames of understanding security research, we understand that while technical security provides useful insights into some aspects of tech abuse, solutions such as policy change or wider awareness of the relationship between violence and oppressive structures such as patriarchy and violence can be more useful. As such, this paper raises questions

[1] We use this terminology as a way of being inclusive in our language. It is a phrase used in violence research to account for peoples' diverse experiences of violence - some may prefer the term victim while others prefer the term survivor as people may be uncomfortable with either.

about privacy and security research and provides pathways for future research.

This paper responds to the need for more nuanced empirical work on existing security practices in the context of services for survivors of coercive control. In doing so, we contribute to privacy and security research in three ways: (1) we expand the field's understanding of technical support by highlighting the ways it is intertwined with emotional and psychological support; (2) using critical and feminist theories, we question conventional understandings of security by adding the notion of care work and relationship-building as integral to the work of security experts; and (3) we redefine technical expertise in security, including knowledge from experiences of on-the-ground support workers and advocates. These theoretical shifts also have more immediate implications privacy and security research, such as a need for more participatory research with practitioners who support survivors of violence, and expanding threat modelling to include interpersonal harms like coercive control and structural forms of discrimination such as misogyny and racism.

Below, we provide an overview of the literature in security and related fields: first, we describe technology-enabled coercive control, second, we outline solutions that have been developed to respond to this kind of violence, and finally, we highlight why it is important to empirically study existing responses to this kind of insecurity. We then present our research methods, including information about our participants and our standpoints as researchers. Following this, we present our findings related to existing support practices, the importance of understanding care as a network, and detail the recommendations for change needed in security technologies and practices that advocates have outlined in the interviews. We conclude with implications for privacy and security research.

2 Background and related work

Conventionally, information security research focuses on defending computer and information systems, and often omits more interpersonal types of harm, abuse, or violence mediated through technologies [57]. Although these forms of tech abuse were seldom discussed in information security research, there has been a recent wave of academic interest in this subject. Most research in this space can roughly be divided into two categories: (1) describing the problem of tech abuse [25, 26, 33, 36, 48], and (2) prescribing, developing, and evaluating solutions that aim to support survivors and prevent abuse [24, 34, 39, 43, 44, 52, 59]. Our study contributes to a third category of work which is often (although not always [19, 65]) omitted: studying and learning from experts who are already addressing this problem by supporting survivors of tech abuse.

2.1 Defining technology-enabled abuse

Technology-enabled abuse describes the deliberate use of technologies or systems to scare, harass, coerce or stalk someone. These forms of abuse are also sometimes referred to as digital or technology-enabled coercive control, cyberviolence, or digital abuse. These terms are often used interchangeably, but they refer to slightly different phenomena. For example, digital coercive control references "coercive control," which is a pattern of behaviour that is designed to assert influence and control over an individual's life using threats of harm, dependence, isolation, intimidation, and/or physical forms of violence, often resulting in a survivor losing a sense of their self-worth, bodily integrity, and safety [19, 62]. Coercive control is increasingly used instead of "domestic violence" to encompass situations in which partners are not cohabitating, as well as to highlight that not all abuse includes physical violence. In contrast, terms like cyberviolence or digital abuse can also include harassment by strangers on online platforms such as Twitter [32, 66].

To simplify the language, we use "tech abuse" as a shorthand for technology-enabled coercive control. This is a broad term that encompass ways in which technology is co-opted for coercive control both in intimate relationships (family or dating violence) as well as violence from strangers which weaponises intimacy or intimate information for coercion and control [44]. For example, technology-enabled stalking or intimate image abuse are harms which are often perpetrated by clients against sex workers [7]. Likewise, harms such as "sextortion," in which the threat of releasing intimate images is used to coerce someone into acts such as sending more intimate images, are sometimes perpetrated by partners or family members, but can also be perpetrated by strangers who specifically target victims on online forums or dating apps [74].

Drawing on past work defining the tech abuse threat model [26, 36, 44, 59, 70], there are five primary forms of tech abuse perpetrators use:

1. Ownership-based access: Being the owner of a device or account allows a perpetrator to prohibit victims'/survivors' usage or track their location and actions;

2. Account/device compromise: Guessing or coercing credentials which enables a perpetrator to install spyware, monitor the victim/survivor, steal their data or lock them out of their account;

3. Harassment: Contacting victims/survivors or their friends, family, employers etc. without their consent, often including deception, defamation or impersonation;

4. Malicious exposure (reputational attack): Sharing or threatening to share private information or non-consensual intimate images (i.e., image-based sexual abuse);

5. Gaslighting: Making a victim-survivor feel as if they are losing their sanity and/or control over their home, for example by remotely changing temperature using an Internet of Things (IoT) device or deleting past messages and denying they were sent.

Perpetrators of tech abuse usually do not use highly technically sophisticated techniques. Instead, since perpetrators are often living with their victims or have intimate relationships with them, they often gain access to victim's accounts through physical access to victims' devices, knowledge of victims' passwords, or their ability to guess or coerce these passwords. As a result, many conventional security measures based on an authentication model, such as passwords and security questions, are not effective in preventing tech abuse. Freed et al. [26] describe the prototypical tech abuse perpetrator as a "UI-bound adversary" who uses the existing interfaces of apps and platforms for abuse, rather than finding exploits in code. When these forms of access are not enough, perpetrators also have easy access to stalkerware programs which enable location-monitoring and other forms of stalking [12]. Such applications are sometimes available on app stores and may even be in-built into our everyday devices, such as 'Find My Friends' or similar location-sharing applications. Other researchers have examined the role of platforms or emerging technology like IoT in mediating abuse [45, 65].

Lastly, a key aspect of defending against technology abuse is that many survivors must live with tech abuse for many years, and so it is often not possible to secure devices and cut off contact. Survivors stay in abusive relationships for many reasons, including financial dependence, legal constraints (such as visa regimes tied to marriage) and the psychological impacts of coercive control. Survivors' privacy and security needs and practices therefore change at various stages of the relationship. Sometimes defending against abuse involves managing living under surveillance, while at other times, for example while preparing an escape, it may involve fully wiping devices to avoid being tracked [34, 48, 71]. Even survivors who are able to leave violent and harmful relationships may have to maintain contact with the perpetrators, for example due to shared custody of children.

These difficulties are further exacerbated and complicated when victim-survivors' identities are tied to multiple forms of oppression. Like all forms of abuse, technology-enabled coercive control is underpinned by societal structures of oppression such as racism, misogyny, class privilege, ableism, heterosexism, and so on [29, 32, 60]. People experience oppression at the intersections of these different aspects of their identity, forming multiple kinds of complex experiences. Because of this, research which focuses primarily or exclusively on the role of gender in harassment and abuse risks marginalizing people who identify with multiple intersecting identities [32]. For example, while women experience domestic and sexual violence at disproportionate rates to men, poor women, women of colour, and immigrant women are also further marginalised when law enforcement do not take these experiences seriously or even penalise survivors of abuse [16, 60]. The majority of existing research focuses primarily on the Global North, mostly including English-speaking countries such as the US, UK, and Australia, and therefore may fail to account for regional and cultural specificities [55].

As a result of such socio-economic, legal, and familial reasons, many victim-survivors must live with tech abuse for many years. In many cases, ending technology-mediated abuse is not as simple as securing devices or changing passwords. Societal issues such as intimate partner violence and coercive control, even when mediated through technologies, cannot be solved with solely technical fixes. Below, we look towards work that has responded to this kind of abuse, providing starting points for addressing this issue within the security community.

2.2 Exploring solutions and recommendations

Following empirical research to understand practices of perpetrators and needs of survivors, researchers turned their attention towards finding solutions. Here, we differentiate between three areas of solution-oriented work: (1) recommendations for survivors; (2) technical recommendations; and (3) the development of services, particularly through community-based action research projects. While it is important for research to explore and recommend solutions, this is not the only way to approach this problem and can in fact miss an important step: i.e., closely studying existing security practices.

Responses to tech abuse, particularly from law enforcement, often include recommendations for survivors to keep themselves safe. These risk imposing an additional burden of "safety work" on survivors who are already psychologically, financially and emotionally burdened by abuse, or creating new forms of victim-blaming in which survivors are accused of having inflicted harm upon themselves by choosing to use certain devices and/or platforms [33, 63].

Technical solutions have included design recommendations [39, 44, 51] and methods such as threat modelling [59], co-design with survivors [43], and usability analysis [52] for the design and development of safer systems. There are also examples that have put into practice some of these recommendations, such as Arief et al.'s [2] platform for survivors, the Tech vs Abuse project [73], or Unmochon, a tool for publicly sharing evidence of harassment [64]. These approaches are valuable, as they highlight the role of technology design in mediating and enabling abuse and offer technology companies ways to address and mitigate technology abuse in design. It is important for companies to understand they have a responsibility to address these problems on their products and platforms. However, problems of abuse cannot fully be "designed out" or "solved" by UX changes [5].

Other solutions have included recommendations of support

systems, such as calls for greater empathy from technologists, police officers, educators and employers [42] and legal and policy recommendations [14]. Alongside academic research, "grey literature" (such as non-academic reports and guidance documents) from women's support services [14], sex worker organisers [31], or organisations working on online gender based violence [28] has also centred the testimonies of survivors, provided timely empirical research about experiences of harm and violence, as well as opportunities for the development of services to support perpetrators in changing their behaviours [3].

Although empirically studying tech abuse advocates' security and safety practices has not been the focus of much existing research, some valuable exceptions include studies of ecosystems of support for tech abuse survivors [25], safety planning practices in domestic violence shelters [49] and the information security needs of human trafficking services [13]. These studies emphasize the difficulties and importance of balancing information security and psychological safety for survivors as well as technology as a "double-edged sword" which both enables survivors and exposes them to risks. Lastly, not all survivors can access conventional victim support services. For example, Sambasivan et al. [55] emphasize many survivors' preference for seeking support from friends and family, and Zou et al. [75] investigate the role of customer support in an anti-virus company in aiding survivors.

Two projects have combined developing solutions with empirically studying the support sector by setting up clinics where technologists support survivors in securing their devices. The Clinic to End Tech Abuse in New York, USA, has described existing ecosystems of support for tech abuse survivors [34], produced resources and checklists for securing survivors accounts and devices [68], and explored the challenges of providing services to survivors during the covid-19 pandemic [71].

The Technology-Enabled Coercive Control Initiative is a community-based participatory action research project in Seattle, USA, in which researchers collaborate with advocates to better understand the problem of technology-enabled coercive control [19]. Their research has both helped define the problem of tech abuse, highlighting how tech abuse can be debilitating and cause feelings of hopelessness in survivors, and also understand gaps and failures in support systems. They emphasize that the process of seeking relief and accountability through civil and criminal legal systems is often ineffectual and can even be retraumatising.

Both these initiatives focus on "building bridges" between the victim-support sector and law enforcement, researchers, and technology companies to more effectively provide relief [19]. These projects have highlighted broader legal and policy changes which must happen to address the rise of technology-enabled abuse: for example, although tech abuse clinics have made significant contributions in local contexts, significant funding and investment would be needed to make these services accessible more broadly [24]. Similarly, a recent study of the intimate partner violence support sector in the UK highlights the shortcomings of existing risk assessment and recording practices as well as the urgent need for greater funding to develop the sector's capacities [65].

To summarise, many researchers have started developing solutions at individual, technical, and societal levels. However, these papers generally do not provide a comprehensive look at what security practices look like in the sector. Instead, they often point towards spaces that require improvement, in what can be called a deficit model for research: looking for what needs fixing, but not looking at innovation that is happening among practitioners and what we can learn from it.

2.3 Examining security and care practices

Taking a closer look at existing support systems allows us to understand how safety is achieved in practice, so that we build on this rather than jumping to providing solutions. This interest in empirically studying support practices is motivated by two theoretical traditions in ethical and political theory: critical security studies and the ethics of care.

Critical security studies places a methodological emphasis on security as a practice as opposed to security as an object or a state [1]. Security practices can include surveillance or predictive policing as well as discursive practices like securitisation, i.e. framing a policy area (like the "war on drugs" or immigration) as a security issue [4, 10]. Critical security theorists are generally sceptical of this process of securitisation, arguing it is used to justify imposing and extending carceral or authoritarian state power [50], as well as technologies that are abusive or cement problematic power relationships [61]. For example, Stahl et al. [61] document how access controls in a hospital computer system cement a hierarchical relationship between patients and doctors that is at odds with the hospital's patient-centred values. Critical theorists often illustrate or deconstruct how ideas about security, as well as practices in which those ideas are enacted, lead to harmful outcomes. Instead of aiming for security, many critical theorists focus on goals like individual and collective emancipation or liberation [23].

Feminist theorists of security studies have long argued that conventional or mainstream notions of security exclude forms of violence that are deemed "personal" or "private", including gendered violence like domestic or sexual violence [56, 67]. Security is often considered at the scale of "high politics" like the UN Security Council, international espionage, or, increasingly, corporate boardrooms rather than everyday life or everyday surveillance [20, 47]. Cybersecurity research has traditionally recreated these patterns of omission by excluding threats like domestic and intimate partner violence from the threat models that inform security analysis [57]. In contrast, Hörschelmann et al. [40] describe social relations as sources of both security and insecurity, or a "key connective

tissue through which different dimensions of (in)security are entangled." They describe security practices as including the emotional and practical labour invested in dealing with the breakdown of social relations.

This reflects a broader focus in much feminist political and ethical theory on the notion of care. In particular, the "ethics of care" is a feminist moral theory which focuses on care as a principle and practice within a wider network of relations between human beings [35]. Theorists in this tradition often posit that experiences of caring for others, particularly those who are vulnerable, give care-provider privileged access to distinctive and valid forms of moral thought [35, 69]. Care ethics emphasize the value and necessity of caring labour as well as the values of empathy, sensitivity, trust, and responding to need.

Black feminists have also championed the concept of self-care, following Audre Lorde's work on self-care as a radical political act for those burdened within oppressive systems [46]. Akiwowo [72] extends these ideas to digital privacy, advocating for "digital self-care" (such as muting abusive words on Twitter) and bystander interventions into online harassment. In the words of Saidiya Hartman, "care is the antidote to violence" [41].

Theorists of care have also introduced critical approaches to care work, focusing for example on the ways in which unpaid care work furthers gender inequalities [37] and how this disproportionately burdens poor women and women of colour [38, 46]. Lastly, some theorists have been careful to highlight the "dark sides of care," noting how care can become a cover for control or be disempowering to receivers of care, for example for people with disabilities experiencing medical care [6].

2.4 Summary

The majority of research on technology-enabled abuse focuses on understanding the problem, including documenting perpetrators attacks and survivors' security needs and practices, or developing recommendations and solutions to the problem. This study however builds on previous literature by examining what existing security practices look like in this field. This is theoretically motivated by critical security studies as well as feminist research on security and care. These theoretical traditions, in their focus on practice, critical approaches to the notion of security, and emphasis on care, have much to offer the study of information security and privacy [61]. Advocates who support survivors of technology abuse are both security practitioners and care practitioners, and therefore offer a valuable perspective on entanglements between care and security. By critically examining security and care practices, we can gain important understandings of what security is and should be.

3 Methods

In this paper, we expand research related to technology-mediated abuse by learning with and from safety advocates using semi-structured interviews and participatory forms of data analysis. Our research is underpinned by a feminist framing of safety and digitally mediated abuse which involves centring of our participants' expertise not just as 'advocates' but also as security experts. Below, we first present details on our interviews and analysis before addressing the issue of positionality in our work.

3.1 Qualitative interviews

To explore advocates' experiences of supporting survivors of technology abuse in depth, we conducted 26 semi-structured qualitative interviews (see table below), each lasting 1-2h. Although most participants worked in the gender-based violence (GBV) sector broadly construed (i.e. organisations with a focus domestic violence, family violence, human trafficking and sexual violence), a few came from digital privacy groups or hacking collectives which had begun to support survivors of intimate partner violence as a part of their advocacy, often as volunteers. Advocates had worked in the domestic or sexual violence sector for an average of 9.2 years. Lastly, several participants were specifically recruited because they support communities like sex workers, refugees, or LGBTQ+ people who are sometimes excluded from the traditional GBV sector [11].

As we are promoting advocates as experts in their field, we wanted to give advocates the chance to be identified by their name and organisation should they choose to do so [17]. Consequently, although participants in the study are pseudonymous by default, participants could also opt-in to use their real name. Asterisks (*) indicate areas where participants chose to use a pseudonym or keep details confidential. Participant names and organisations are listed in Appendix 1 (7.1).

Participants were recruited using purposive sampling: some were recruited through the first authors' personal network, while others volunteered after the call was shared on a variety of mailing lists aimed at people in the victim support sector. Selection criteria were having supported at least three survivors of technology-facilitated abuse. Interviews were recorded and transcribed using Word Transcribe, and then played back and corrected. Interviews took place over three months from December 2020 to February 2021 and were not compensated.

We asked participants about types of technology abuse they had seen, how they supported survivors, and what improvements they would like to see in technology and cybersecurity. Participants were also prompted to share specific cases, without identifying details, to illustrate how they supported different survivors. We also asked about how participants addressed the psychological distress which survivors experi-

enced as a result of tech abuse, as well as whether there were any demographic factors (like gender, race or immigration status) particular to the survivors they supported that shaped their experience of tech abuse (see 7.2 for the full interview protocol).

3.2 Data analysis

Following the interviews, we hosted a 2h-long workshop to discuss the role of technology-mediated abuse in the development life-cycle of data-intensive technologies [2]. Ten interviewees were invited to this workshop, although not all of them were able to attend. As part of this workshop, we carried out a 'data walkthrough' where we presented our initial data analysis back to participants, asking them to critique our interpretations. We used an interactive whiteboard to support the discussions in the virtual workshop. This allowed participants to add their thoughts and reactions without words. We presented some initial findings from the interviews on the whiteboard, giving participants an opportunity to respond and push back on our interpretations verbally, as well as with post-it notes, emoji, or other forms of visual media on the whiteboard. This process of participatory data interpretation allowed us to conduct research in a less hierarchical way, following feminist principles of participatory research [27]. In particular, we highlighted in the transcript and our findings moments when participants pushed back or re-framed some of our interpretation. The workshop was audio recorded and transcribed; we took screenshots of the whiteboard.

The interview and workshop transcripts were analysed using reflexive thematic analysis [8]. This is an approach to qualitative analysis which emphasizes the active role of the researcher in the knowledge production process and intentionally does not include a codebook or quantification of frequency of themes. Instead, this work focuses on the reflexive development of understanding with and through the data: initially the first author coded the interview transcripts, from which they developed themes. These themes, alongside quotations from the transcripts, were fed back on by participants during the workshop. The transcript from the workshop was then coded and discussed by both authors. As such, the final themes presented in this paper were negotiated between both authors, in conversation with participants, and based on data and our interpretations thereof [9].

In September 2021 the authors worked together to produce a toolkit to improve the safety of people for technology developers and researchers who work closely with data-intensive technologies. This writing process helped crystalise themes and helped further develop our thinking. This learning also feeds into this paper.

[2]The workshop results are described further here: https://nrl.northumbria.ac.uk/id/eprint/47508/

3.3 Ethics

This study received ethical approval from the University of Oxford Central University Research Ethics Committee. We obtained informed consent from participants to conduct and (optionally) to audio record the interview. As the interviews could touch on sensitive topics, we ensured that participants knew that they could skip questions and request a break at any time. We also emphasized that participants should provide only as much detail in their answers as they felt comfortable with. All electronic files were password protected and stored in a secure location.

3.4 Positionality

Both authors are white women feminist researchers in the United Kingdom whose research interests are related to safety and technology. The first author is a PhD student with some experience volunteering with a sexual abuse and rape crisis centre in their listening services, i.e. phone and texting support. This experience allowed for a degree of shared understanding and empathy with participants. The second author is safely employed at a university with experience of working with a number of support services who work with people of all genders who have experienced different forms of interpersonal, politically-motivated, and institutional harms. The two authors bring their experience and gained understanding from their volunteering and collaborative research to frame the concerns outlined in this paper. As such, our feminist approach, the centring of our collaborators' knowledge, and our somewhat-insider knowledge plays a crucial role in our analysis of the data.

4 Findings

In this section we address three main areas: (1) advocates' support practices; (2) the networked and relational forms of security that are produced in this process; and (3) the changes that these advocates propose in how we address tech abuse.

4.1 Support practices

Advocates described supporting survivors in five main ways: by establishing trust and belief; safety planning (which includes threat assessment, resilience mapping, and taking action to secure accounts and devices); empowerment and demystification; supporting evidence-collection and making referrals. While some of these support practices—like threat assessment or securing devices—resemble established cybersecurity practices, others—like demystification—are more nuanced emotional or psychological practices which fall outside of conventional security frameworks.

Establishing trust and belief. Many advocates described establishing trust and belief as a critical prerequisite to pro-

viding any support. In our interviews, many stressed the importance of establishing a relationship before any probing questions about the abuse or survivors' devices were asked. Many survivors will have experienced gaslighting, an abuse tactic in which a perpetrator tries to undermine a survivor's perception of their own sanity. This is then often compounded by disbelief from friends, family, or law enforcement [36]. Natalie Dolci, (Technology-Enabled Coercive Control Initiative [19]) said, "it's very easy for [...] female identified survivors or gender nonconforming survivors [...] to be treated like they're crazy." Consequently, belief and validation–i.e. making sure survivors felt that their concerns were affirmed and taken seriously–were critical principles for the majority of advocates interviewed.

One advocate described doing this through sharing her own experiences of technology abuse to reassure survivors that they are not alone in their experience and "build rapport" with them (Stephanie*). Many others repeated the importance of reassuring survivors that they believed them, that their experiences and emotions were not uncommon, and that they were not to blame for what had happened. Sol*, an advocate who had a day job in white hat hacking, contrasted these practices of belief and validation with "a more anxiety causing ... tendency to talk about the worst case scenario and focus on that" among information security professionals. Practices like establishing trust, building rapport and proactively communicating belief are important prerequisites to creating an emotional sense of safety, before beginning to assess technical device security. This is important because without that trust, advocates might never be able to understand how they can support survivors.

Safety planning. A variety of practices including (1) threat assessment, (2) resilience mapping, and (3) digital self defence–grouped under the term "safety planning" form a major part of the support advocates offer survivors. One way of understanding this is that safety planning is the most obvious substantive form of support, while the other practices outlined in this section are more subtle underlying practices intertwined with safety planning.

Firstly, after establishing trust, advocates often described conducting a formal or informal threat assessment (although most advocates did not describe this in terms of threat assessment). Assessing threats can include technical support like checking devices and accounts, but it can also be assessing for emotional, physical, or financial threats. Chris described this as a "kind of triage, like what do we need to take care of?". Recognising technology abuse alongside other forms of coercive control can be a challenge; several advocates reported that many survivors do not realise that technology abuse is happening as "it's not always very obvious" (Amy Jacques). In particular, advocates emphasized the importance of paying attention to children's accounts and devices in threat assessment, as these can easily be abused. In many situations, survivors may not identify an abusive situation as abusive.

For example, Emma Pickering (Refuge UK) described a situation in which a survivor reported intense harassment of around 100 emails a day, but the police were not taking the case very seriously. Emma went through "a checklist with [the survivor] and it turned out that actually the whole house was rigged with technology. She'd been with him since she's 15 and she thought it was very normal because of the way he behaved to have webcams in the bedroom, the bathroom; he had three home built PCs for the children, the Xbox was rigged." In this case, the survivor was aware of the cameras but had not articulated this behaviour as abuse and therefore did not report it to the police.

Threat assessment practices can come into tension with the principles of belief and validation. For example, Sarah explained "we always want to make sure that we're believing people, but I think for people who may be new to [...] working with someone who's experiencing stalking behavior, especially if that stalking includes tech-facilitated abuse that they may jump to like the zebra issue instead of just working with horses first." She explained this meant both survivors and advocates may assume stalking is related to "more advanced" forms of abuse like spyware or hacking, when in reality, more mundane acts like guessing or coercing a Facebook password are much more common forms of compromise.

Identifying what's possible requires a detailed knowledge of account compromises, such as the fact that if someone has access to an email password, they can likely use that to reset your Facebook password, but not vice versa (Rowan*). Therefore, threat assessment often requires both fairly sophisticated technical knowledge (i.e. differentiating between spyware or various password compromises) as well as the very subtle skills of belief and validation discussed earlier. Advocates take great care to avoid invalidating survivor's experience of abuse, even if their assessment of the problem is different to the survivor's.

Many advocates reported incorporating the framework of intersectionality into their safety planning practices. They confirmed that tech abuse, like other forms of abuse, disproportionately affects people experiencing multiple forms of oppression. For example, survivors with disabilities who rely on assistive technology like mobility aids or screen-readers are particularly vulnerable to that technology being withheld or exploited (Natalie Dolci). Migrant survivors face specific risks like perpetrators impersonating immigration officials online and threatening deportation or threatening to expose undocumented status online. Similarly, Metzli Mejia, (Los Angeles LGBT Center) described how LGBTQ+ survivors face additional risks of being outed online. Lastly, many advocates reported that law enforcement are often less likely to treat cases involving women of colour or those from less wealthy backgrounds seriously. When taking these overlapping identities into account in threat assessment, advocates incorporate intersectionality into their practices.

Secondly, in the data walkthrough, Toby Shulruff made an

important point in noting that advocates do not just assess threats, but also help survivors map their strengths and resilience. Toby noted that there is a tendency, especially in legal systems, to portray survivors as "fragile and in need of saving" when in reality they are highly creative and resilient. By mapping these strengths, advocates help survivors keep in mind all the resources they have to draw on; this is a critical part of empowerment, a practice explored in the next section.

Lastly, safety planning involves taking action to secure accounts and devices, as well as anticipating future scenarios and planning appropriate responses with the survivor. Safety planning was, in advocates' accounts, often closely linked with "survivor centric approaches" which means "deferring to what the survivor identifies as best outcome" (Sarah). For example, rather than pressuring survivors to leave, advocates reported changing their advice and safety planning to adjust to the survivors' preferences.

Besides securing accounts and devices, safety planning may include actions like limiting social media use, or dating app use, reporting perpetrator to social media platform, or forwarding emails from the perpetrator to a separate folder to limit time spent engaging. Many of these resemble what Akiwowo [72] described as "digital self care". Farah Sattar (DCRYPTD) described these as general "digital self defence" techniques.

Advocates were careful to highlight potential unintended consequences to survivors: for example, removing spyware might result in losing the evidence that it was there in the first place. The difficulties of evidence-collection will be explored further in 4.1. Furthermore, removing a tracking app from a survivor's phone may result in further violence and abuse from a controlling partner, rather than making them safer. This is why it is imperative to incorporate the survivor's experiences, needs, context, and preferences into any advice.

Demystification and empowerment. Throughout supporting survivors who experience tech abuse, advocates seek to empower survivors to recognise their strengths while simultaneously demystifying the disproportionate power perpetrators attempt to project. As Eva Galperin (Electronic Frontier Foundation) said, "for a lot of people, technical knowledge and you know computer security is essentially magic [...] so it's very easy to use the appearance of that knowledge to make yourself seem omniscient and omnipotent and often that alone is enough to manipulate the victim." Similarly, Chris said "a lot of times the abuser is promoting themselves as this tech god and they create an impression of themselves as just being all knowing and they can do anything." This overstating of perpetrator capabilities complicates threat assessment, contributing to the zebra vs horse problem described above. Advocates will demystify this appearance of power by helping survivors understand "what the perpetrator is actually capable of, and what's bullshit" (Eva Galperin).

Drawing on research from the Technology-Enabled Coercive Control Initiative [19], Natalie Dolci phrased this in terms of "perceived expert status": perpetrators will often overstate their "tech-savviness" and advocates try to diminish this perceived expert status while raising survivors perceptions of their own expertise and technical competence.

At the same time, advocates will both help survivors develop their technical skills and recognise how many technical skills they already have, in a process of empowerment. For example, Adam Dodge described asking survivors if they "know how to reset a password, know what location tracking apps are and what they do, know what Wi-Fi is" and when they answered yes, saying "I would describe that a person who knows how to use all those things and knows what they are as actually very tech savvy." Similarly, for many advocates even mundane processes of threat assessment were phrased in terms of empowerment: for example, describing how to distinguish between annoying adware and targeted attacks as helping people "to be more empowered" (Toby Shulruff).

Survivors experience feelings of helplessness and disempowerment as a result of tech abuse, which limit their liberty [19, 62]. This makes it particularly critical that advocates' security practices are based on empowerment as well as belief and validation. The technical support and advice advocates give needs to be survivor-centric and respect survivors agency in order to avoid repeating patterns of coercion and control. By improving survivors' perceptions of their own technical expertise, while simultaneously reducing the perpetrators perceived expert status [19], advocates aim to create a sense of safety which is synonymous with empowerment.

Supporting evidence collection. Although most advocates we interviewed were not lawyers, guiding and supporting survivors through interactions with law enforcement and court systems was a huge part of the work advocates described. Documenting device compromise, abusive messages, or oppressive surveillance are critical for seeking redress through legal routes, such as reporting to law enforcement, getting a restraining order, or going to court.

Advocates supported this using tools such as "stalking logs" which allow survivors to record unwanted contact and interactions with perpetrators (Stephanie*). Advocates also often mentioned screenshots as a critical tool for producing evidence. Two advocates also described recommending a specific app called Our Family Wizard which is sometimes prescribed in court orders for co-parenting. Both advocates said this app was for making it easy to print a log of all text messages, phone logs and emails to provide to a court (although other advocates also expressed reservations about the way courts mandate it).

However, collecting evidence can often be very tricky. Many advocates noted the difficulties of procuring a record from private platforms like Facebook or Snapchat. Rebecca* described a particularly frustrating pattern with non-consensual intimate images shared on Facebook: "if you don't screenshot them before they're taken down, then it's really difficult to get information from Facebook, like get evidence

of it for court." Getting tech companies (usually based in the US) to respond to requests for evidence is often even harder in countries outside the Global North: Andrijana Radoicic Nedeljkovic, an advocate at Atina, a human trafficking and domestic violence shelter in Serbia, described a case where the state prosecutor had to wait thirteen months for a response from Facebook.

In addition, judges often do not know how to interpret technical data relating to forensics. Likewise, law enforcement often do not have the necessary skills to collect evidence and preserve evidence, so that skilled defence lawyers can make "technical legal arguments around [...] in relation to the chain of evidence" (Milcah*). With harassment using anonymous platforms or spoofed phone numbers, attribution and demonstrating authenticity is a challenge. Because it is hard to "get physical proof that it's happening", tech abuse often is not "taken as seriously by different systems" (Rowan*). Hera Hussein (Chayn) tied this to "a hysteria amongst the [criminal justice profession] around women submitting false cases." Ben Walker (Tech-Enabled Coercive Control Clinic), described being unable to help survivors by providing evidence in court as then "our clinics records could become public as a result of subpoenas."

Technical capacities for collecting evidence can also themselves be abused. Hera Hussein described a case where a woman was recorded for ten years in her home by her partner without her knowledge. Her partner was now using those ten years of security camera footage against her to fight a custody battle by selecting footage that suited his case and omitted evidence of his own behaviours. In this case, part of the support Hera was able to offer was to help the survivor validate her experience of being secretly recorded as coercive control: "you start peeling the layers that society has, like you know, put on women's minds about compromise and understanding the other person and they start seeing the situation for what it is. I think that is a very heavily underappreciated service to support survivors' understanding."

Supporting evidence collection is critical in criminal and civil legal systems, in all countries in which we interviewed advocates. Evidence can also be very psychologically important in the context of gaslighting, so survivors can be reassured their experiences are valid. Therefore, evidence collection, although it is not immediately related to securing devices, is crucial for accomplishing a broader sense of safety and security.

Referrals. Lastly, advocates support survivors by connecting them with various specialists, resources and other support services. As Susan Hickey (Harris Country Domestic Violence Coordinating Council) said "we're kind of like [...] a bridge to other resources." In order to be able to refer survivors to these services, advocates first need to build networks of people who can be trusted to support survivors. This practice of developing and maintaining networks of care will be explored further in the next section.

4.2 Networks of care

Networks of care are networks of practitioners willing and able to support survivors with specific needs. Developing and maintaining these networks is a critical security practice that advocates do in order to create more supportive and caring environments for survivors, and in many ways a prerequisite to the individual support practices described in the previous section. The following section first describes the key attributes of these networks, and then explores two particularly tricky relationships to maintain: namely, with law enforcement and tech companies.

4.2.1 Defining networks of care

Networks of care have three key attributes: namely, they involve elements of care, education, and relationships. Firstly, these networks' purpose is to create caring environments for survivors. This support is often not just about pragmatic advice but also about showing care. For example, several advocates mentioned making connections with very local contacts, such as "Geek Squad" tech support services at an electronics store, or a local car mechanic. Susan Hickey explained, "I really like when car companies will say yeah, sure I'll come and I'll look at your car [...] Maybe they're not going to see everything. But I think it just provides a survivor that support that's so important to know that there are people that care." As survivors have often experienced isolation and cruelty from perpetrators, as well as indifference or ignorance from legal systems, building experiences of care is crucial.

Secondly, building links in the networks of care often involves educating various stakeholders in order to prevent those actors from invalidating survivors' experiences in ways that contribute to gaslighting. For example, Susan described wanting to make sure a counsellor was "aware of all the ways a person could [...] use technology to abuse them [...] so they're not [...] like oh lady, you're crazy." Similarly Rebecca* mentioned, "if there were say like a IT expert who could go through their phone with them but was not trauma informed, I would be nervous to refer someone to that person without also being there." A particular risk for advocates coming from the digital privacy or cybersecurity space is "judging [survivors] very harshly, scaring them, giving them advice that is meant for protecting them from nation states or law enforcement rather than their [...] abusers level of technical skill" (Eva Galperin). Therefore, building these networks is more complicated than simply identifying local services; advocates must also ensure that other actors in their network will take a caring, trauma-informed approach.

Lastly, the work of developing networks of care is highly relational as they require building and maintaining relationships. The emotional labour that goes into developing these networks–for example, anticipating how an IT expert may invalidate a survivors' experience–is not commonly appreciated as a kind of security work.

4.2.2 Law enforcement

Advocates described a complicated relationship with law enforcement: they have to rely on the police to conduct investigations and enforce protection orders, while simultaneously trying to mitigate the many ways legal systems fail to address cases of partner and family violence. Andrijana Radoicic Nedeljkovic (Atina) described the risk of law enforcement not treating tech abuse like "real violence" which can create a confusing situation of "double messaging" for survivors after advocates have encouraged them to identify their experiences as abuse. For this reason, for many advocates it is important not just to support survivors in articulating abuse, but also to educate law enforcement to be more receptive and understanding.

Although many advocates described the importance of maintaining close relationships with law enforcement to ensure perpetrators are prosecuted, many also emphasized that "the vast majority of survivors don't report to law enforcement, don't want to be involved in legal systems for a full variety of reasons, or they approach legal systems, and legal systems aren't able to [help them]" (Toby Shulfuff). As a result, most advocates agreed that the main source of support for survivors should "stay with NGOs and community based organizations" (Toby Shulruff). Law enforcement is often implicitly assumed to be a solution to coercive control and domestic violence, yet it is often a part of the problem. Advocates are therefore an alternative source of security to that practiced by courts and police.

4.2.3 Tech workers and tech companies

Another significant group that advocates described building relationships with were tech companies and tech workers. Advocates often described a serious gap in support and care from large tech companies. Many advocates had reached out to tech companies and reported a variety of frustrating experiences. One advocate said, "computer emergency response teams at companies do not want to tackle tech abuse." Several advocates noted that it is impossible to get any form of human customer service from large platforms like Facebook or Twitter, "these monolithic companies that have no telephone number or they have no email address" (Chris). Even in very serious stalking or abuse cases, survivors must navigate complicated forms and help pages without support. "The ability to reach a person would be a game changer" particularly if there were "customer service people who specialised in identifying and supporting survivors of intimate partner violence" (Natalie Dolci).

This gap in support is being filled by tech advocates, often in ways that creates burdens for their organisations. As one advocate said, "the tech companies' lax attitude to customer service is remedied by people in the advocate/charity space, without compensation." Luiza* described an (ongoing as of time of writing) situation in which Pornhub, without seeking or getting permission, links to her organisations' Facebook page on its "Non-Consensual Content Policy" website, which results in thousands of people from all over the world reaching out for support with cases of image-based sexual abuse. The advocate spent an increasing amount of her time helping people navigate Pornhub and other platforms, like Facebook's, non-consensual content policies. She said "the thing that's really disheartening and upsetting, is that, you know, someone reaches out to me to support them. Like immediately [...] like I'm really going to be like [...] Okay let me just get Mark on the phone quickly and I'm like yo Zuckerberg [...] take this down quickly." This is challenging as it often takes weeks to get non-consensual content removed, and then when it is removed, there is no support for getting evidence to prove it e.g. in a court of law. As a result, she said "It's like I don't have the funding anymore to do this work and I can't stop either right? [my supervisor suggested] it's an emotional strain to support people, right? And it's not like- this isn't my role [..] I'm not a trained counsellor."

In the data walkthrough workshop, we suggested that companies like Facebook or Pornhub should be providing more support to survivors, as it seemed the advocate in the situation above was doing unfunded customer support for these companies. Interestingly, this was partially challenged by Kate Worthington, a practitioner working with the Revenge Porn Helpline, who said, "I don't think I would trust the tech companies to take on that emotional support." She highlighted the importance of having support from independent organisations, as customer support services inevitably have the company's interest, which often differ from the survivors' in mind.

Similarly, Eva Galperin described experts in forensics reaching out and offering to help her with the work she does supporting survivors, and said "the problem with that is that my backlog is not technical, my backlog is therapeutic, my backlog is in [...] trauma informed approach and I usually cannot trust the technical people who approach me to know how to do any of those things, and so usually they are appalled when my response is a reading list." This highlights the enduring importance of funding independent support services, alongside calling for better support from companies. Further recommendations for change will be explored in the next section.

4.3 Recommendations for change

In the previous two sections, we have highlighted advocates expertise in combining technical and emotional support practices as well as developing networks of care. In our interviews, advocates also made a variety of recommendations for how to address the problem of technology-facilitated abuse. These recommendations are important because, as advocates are not widely recognised as tech experts, their ideas for how to improve technology safety usually have not been included in privacy and security discussions.

Participants in the study emphasized that more support and funding for training in building capacity is needed. This echoes a general concern with insufficient funding and resources in the field [19, 65]. Some argued it would be more sustainable to develop more partnerships and collaboration with digital security practitioners. This applies also to the digital privacy and rights space: advocates noted that many online privacy resources are directed at politicians, activists and journalists and not domestic violence survivors.

Advocates also made a variety of recommendations for improving technology design. Many of these related to higher levels of privacy and security by default, such as setting a notification reminder to periodically prompt deletion of location data (Ben Walker), or sending notifications when someone logs into your account from a new device.

Others made recommendations related to content uploads and moderation. Companies are often incentivised to coax users to upload as much engaging content as possible at the cost of safety. Advocates called instead for practices which prioritised consent and mechanisms for removing harmful content over data collection and engagement. For example, one advocate suggested, "the upload button on websites needs to be the same size/prominence as the report button" (data walkthrough). Others emphasized the importance of having these reports read "at the same quick speed it is to upload the content" (data walkthrough). Andrijana Radoicic Nedeljkovic suggested that platforms could use facial recognition to notify people when someone uploads a photo of them, and to "be sure that the person had given consent." Mechanisms for reporting could also be much more trauma-informed. For example, when reporting on forms and websites, survivors often are not informed about outcomes, so "you don't get that validation. You know it's all just like, well, you've made this report allegation thing, and we'll kind of have our own really opaque internal process about what's going to happen. So that is not very survivor friendly or validating" (Toby Shulruff). By understanding what good support practices (outlined in the previous two sections), companies can create better support mechanisms for survivors.

Many recommendations for technology design related to broader processes and practices at tech companies rather than specific UX changes. Advocates showed awareness that product design related to the design process, saying "access to information about your physical location through Find My Friends [...] usually has its roots in design. User design that is not designed to take the abuse case as a use case." Advocates suggested incorporating tech abuse into conventional security practices like threat modelling or maturity models, saying "perhaps there needs to be some sort of maturity model related to trauma-informed care for companies just as they would have for other issues."

Natalie Dolci called for "a relational dynamic between victim service organizations where we can say, hey, these are the concerns we've seen this past quarter on your platform." This would allow victim service organisations to flag problems as they arise. This was contrasted with disregard or tokenistic inclusion by companies, in which survivors or advocates were only asked for "green stamp" approval on solutions which had already been developed.

Lastly, Luiza* called for more company measures aimed at perpetrators rather than survivors: "all these platforms can target advertising at a particular person [...] they know that I like ice cream and I'm in the neighbourhood and boom, there's a coupon that's going to come directly to me on a hot summer day. [...] why can't they use the same resources and tools to direct public awareness messaging at perpetrators?" This echoes calls in the literature like [3] to shift the responsibility for addressing tech abuse from survivors to perpetrators.

Advocates recommendations for addressing tech abuse included more funding and resources for capacity building in law enforcement and the support sector, product design in which safety and security are built in by default, and better responsiveness when advocates and survivors raise problems. These recommendations are grounded in an understanding of security as networked and relational: in order to adequately respond to the evolving problem of tech abuse, tech companies and security workers need to develop respectful relationships with advocates working on these problems on the ground.

5 Discussion

This paper responds to the need we outlined in section 2 to study existing safety strategies to support victim-survivors of technology-facilitated abuse. In section 3, we present safety practices of individual advocates as well as how this work is situated in and promotes the development of wider networks of care which incorporate different kinds of expertise - including that of people within the security sector.

However, to fully empower survivors, we would require a destruction of patriarchal social structures and the provision of adequate housing for survivors, social services support, and a variety of other support measures which are not new technologies. This is not an issue that the security community can tackle on its own. However, there are ways in which the work that takes place within the community, especially that which aims to address the topic of technology-facilitated abuse and/or other forms of violence against marginalised people, can better support safety work. We have already presented pragmatic advice from advocates directly in section 3, and now expand with more high-level suggestions for the security community: (1) the need to redefine technical expertise; and (2) the need to recognize networked care work as central to security work.

5.1 Redefining technical expertise

As we outlined in 2.3, theorists in the framework of the ethics of care posit that experiences of caring for those who are

vulnerable give care-providers access to distinctive insights on ethics. We follow and extend this tradition, showing how experiences of supporting survivors lead tech abuse advocates to develop valuable expertise on technology and digital security. Advocates in this space have developed a unique set of skills that combines technical knowledge with the emotional and therapeutic sensitivity needed to support people who have experienced trauma.

This finding departs from several existing studies of the tech abuse support ecosystem which highlight gaps in training and capacity in the sector, sometimes presenting support services as overwhelmed or ill-equipped to address the problem of technology abuse [19,65]. For example, a recent study [65] concluded that "both statutory and voluntary sector representatives 'don't want to be tech experts' [...] nor should they have to be." In fact, some advocates we interviewed also did not consider themselves to be "tech savvy."

This seeming inconsistency can be partially explained by our recruitment and well as through self-selection of participants. Unlike previous studies, we spoke only to advocates who were already interested in and knowledgeable about the problem of tech abuse. Their level of technology expertise is not necessarily representative of the broader community of practitioners in support services.

However, this tension is also linked to our desire to reframe what is commonly understood as technical expertise. Not every support worker in the field of domestic and sexual violence should necessarily be viewed as a technology expert, yet each of them, including those who did not consider themselves tech savvy, will have valuable experience with understanding the dynamics of coercive control, as well as how technology can enable these dynamics.

For example, advocates consider intersecting systems of power and oppression, like misogyny, racism, or ableism, in their threat assessment; these factors should be considered in threat assessments more broadly. Similarly, ideas such as focusing on the "horse issue" instead of the "zebra issue" (see 4.1) are valuable for academic research and media reporting, which can fixate on flashy, sophisticated, but relatively rare, attacks like spyware and omit mundane and common attacks like coercing Facebook passwords. Advocates practices of belief, empowerment, and demystification, also point to the intertwined psychological, emotional, and technical aspects of information security.

Tech abuse advocates' expertise departs from conventional understandings of a "cybersecurity expert" which might involve someone with in-depth knowledge of cryptography or malware analysis. However, this expertise is incredibly valuable for understanding online safety and security. This expertise should be recognised by technology designers and companies looking to build safer digital systems. Many of these organisations also need to receive much better funding from government institutions to continue doing the important work that they do. Therefore we absolutely support calls for greater funding and training to extend the capabilities in the victim support sector, however we also want to highlight that this grounded knowledge translated into many valuable insights which the digital privacy and security community can learn from.

In order to integrate this new understanding of technical expertise, those developing and deploying technical systems should seek out and, crucially, compensate advocates who have direct experience with the harms their products can cause. Practitioners who work on the ground with people directly affected by the problem are a critical source of security expertise. This is true not just for the problems of technology-enabled coercive control or domestic violence, but also more broadly for other forms of abuse or discrimination that are exacerbated by technology, such as racism or xenophobia.

Likewise, security and privacy researchers should collaborate with such practitioners by employing participatory research methods such as those applied by tech abuse clinics [19,34] or in "participatory threat modelling" [58]. Threat modelling both in research and in industry practices should include interpersonal harms such coercive control, bullying, or stalking [26,53,59]. Incorporating the perspectives of both survivors of violence and practitioners who support them will help address blindspots in threat modelling and develop more robust security practices [59].

5.2 Networked care as central to security

Advocates work to create safety for survivors through empowerment, validation, and creating networks of caring, supportive people that survivors can rely on for support. Many of their practices (like threat assessment and safety planning) do resemble conventional security practices. However, practices like advocating for digital self-care or empowerment through technical skills clearly relate to digital security, yet extend far beyond ensuring technical security of accounts and devices. These kinds of care work more closely resemble what Hörschelmann et al. [40] describe as "webs of (in)security" or security practices which include the emotional and practical labour invested in dealing with the breakdown of social relations. It remains an open question whether it is more helpful to reconceptualise (some) care practices as security practices or move away from the notion of security entirely. In fact, advocates themselves rarely used the word "security", often speaking of "empowerment" instead.

This is reminiscent of critical security theorists' preference for emancipation or liberation over security. Critical security theorists emphasize that some security practices can be harmful, as when practitioners in the security industry will inflate threats to sell security as a product [50]. This form of tech saviourism can be disempowering or even exploitative to security subjects, exposing them to surveillance in the name of security, or leaving them in a permanent state of fear. Advocates supporting survivors are not in a financial relationship

with survivors and do not need to sell them security products (as security practitioners in a company may be). Crucially (as described in section 1.3), through their focus on empowering survivors and demystifying abuser's abilities, tech abuse advocates actually invest a significant amount of time and energy to reduce perpetrators' perceived expertise. This runs counter to many security practices of threat inflation which are critiqued within critical security studies.

Tseng et al. [71] have noted that the language of "empowerment" can be misleading in this context, arguing that tech abuse support practices are better described as enablement, or the facilitation of "opportunities for people to develop their own capacity." As Erete et al. [21] write, technology interventions alone cannot empower people without addressing underlying social, economics, and political inequities. Survivors are often targeted because they belong to a systematically marginalized group and abusers know they can wield power against them. To describe projects and technologies as empowering when they do not truly shift these underlying power structures can obscure this reality [71]. Although we cannot evaluate to what extent these practices are actually empowering, the fact that these advocates actively aim for agency and empowerment as a part of security is still significant, as it runs counter to many descriptions of security practices within critical security studies.

Privacy and security researchers and practitioners can draw several insights from the findings and questions raised in this paper. Firstly, by learning about digital security practices in a very different context from the standard security setting (i.e., within a corporate or military organisation) security practitioners can reflect on their own security practices: for example, advocates actively incorporate the values of empowerment in their practices. What kind of values do security practices in other contexts incorporate?

Secondly, this study highlights the benefits of studying existing practices rather than prioritising the development of new technical solutions, offering a pragmatic alternative to technical solutionism. Having an awareness of security as a set of practices opens up the possibility of understanding the networks through which these practices take place. Practices such as developing networks of care in communities are a critical source of support for survivors of abuse and easily missed if the focus is solely on securing devices.

5.3 Limitations and directions for future work

In looking closely at advocates' support practices and exploring their understandings of security, we have accepted a variety of limitations which would have enriched our work and are important to explore in further research.

First, we focused our research design on interviews with advocates, not survivors (with a few exceptions where advocates had themselves experienced technology abuse) so we did not assess survivors' perspectives on these support systems. Therefore, we were only able to describe support practices as they were related to us by advocates; as with any practice, there is likely a gap between what practitioners describe and how this works in practice. Methods such as ethnography and participatory observation, as well as interviewing survivors about their experiences, would provide a richer picture. Survivors' experiences of abuse have been a significant focus of research [25,48], but their experience of support practices and their ideas about safety would undoubtedly be very valuable for future work.

More broadly, we do not fully engage here with existing debates on accessibility and inclusiveness within the field of coercive control and gender-based violence. For example, as a result of the severe isolation that often comes with abuse, many survivors are not able to access support services in the first place, while others have reported negative or exclusionary experiences at support services [60]. Scholars and practitioners advocating for abolitionist perspectives argue that close relationships between domestic violence services and law enforcement are a barrier to access for marginalised groups who are disproportionately targeted [18, 60]. Additionally, others are concerned that a sector originally developed to support "battered women" does not adequately support male, LGBTQ+, trans or non-binary survivors of abuse [11, 22, 30, 54]. These issues are contested and complex, and warrant further study to see how they intersect with privacy and security concerns.

6 Conclusion

Advocates who support victim-survivors of technology-facilitated abuse are (often un-acknowledged) cybersecurity workers and experts. Through their work in developing safety strategies and the sustainable establishment of networks of care, these advocates reconfigure cybersecurity as a form of care sensitive to the experience of trauma. With this paper, we expand the security and privacy community's understanding of this kind of work, and how it can be adapted into security research practices. We do this by (1) expanding the field's understanding of what 'technical' support in security studies is and could be, adding layers of care and relational support; (2) questioning conventional understandings of security by adding the notion of care work as integral to the work of security experts; and (3) redefining technical expertise in security, including knowledge from experiences of support workers and advocates. To better support victim-survivors of technology-mediated abuse, we argue that the security community must re-evaluate its understanding of technical expertise to validate and incorporate the expertise of advocates, and recognize the individual and networked care that is inherent to this work. Once we recognise and understand these networks of care, we can build on and extend them though employing participatory methods and expanding threat modelling to account for harms like coercive control and structural forms of discrimination.

Acknowledgments

Many thanks to our participants, without whose ideas and dedication this work would not be possible. Thank you also to Helena Webb and Gina Neff for invaluable supervision and support. Parts of this work were funded by the EPSRC EP/R045178/1 Human Data Interaction: Legibility, Agency, Negotiability' and the EPSRC Studentship as a part of the Oxford Centre for Doctoral Training in Cybersecurity.

References

[1] Claudia Aradau, Jef Huysmans, Andrew Neal, and Nadine Voelkner. *Critical security methods: New frameworks for analysis*. 2014.

[2] Budi Arief, Kovila P.L. Coopamootoo, Martin Emms, and Aad Van Moorsel. Sensible privacy: How we can protect domestic violence survivors without facilitating misuse. *Proceedings of the ACM Conference on Computer and Communications Security*, pages 201–204, 11 2014.

[3] Rosanna Bellini and Alexander Wilson. Fragments of the past: Curating peer support with perpetrators of domestic violence. *Conference on Human Factors in Computing Systems - Proceedings*, 5 2021.

[4] Valeria Bello. The securitisation of migration in the eu: debates since 9/11. *Global Affairs*, 2, 2016.

[5] Mark Blythe, Kristina Andersen, Rachel Clarke, and Peter Wright. Anti-solutionist strategies: Seriously silly design fiction. *Conference on Human Factors in Computing Systems - Proceedings*, pages 4968–4978, 5 2016.

[6] Liz Bondi. On the relational dynamics of caring: A psychotherapeutic approach to emotional and power dimensions of women's care work. *Gender, Place and Culture*, 15, 2008.

[7] Raven Bowen, Scarlett Redman, Kerri Swindells, and Tess Herrmann. Sex workers too: Summary of evidence for vawg 2020-24 consultation. 2021.

[8] Virginia Braun and Victoria Clarke. Reflecting on reflexive thematic analysis, 2019.

[9] Virginia Braun and Victoria Clarke. One size fits all? what counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, 18(3):328–352, 2021.

[10] Barry Buzan and Ole WÆver. Macrosecuritisation and security constellations: Reconsidering scale in securitisation theory. *Review of International Studies*, 35, 2009.

[11] Jenna M. Calton, Lauren Bennett Cattaneo, and Kris T. Gebhard. Barriers to help seeking for lesbian, gay, bisexual, transgender, and queer survivors of intimate partner violence:. *http://dx.doi.org/10.1177/1524838015585318*, 17:585–600, 5 2015.

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

[13] Christine Chen, Nicola Dell, and Franziska Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. pages 89–104. USENIX Association, 8 2019.

[14] Danielle Keats Citron. Sexual privacy. *Yale Law Journal*, 128, 5 2019.

[15] Lizzie Coles-Kemp, Debi Ashenden, and Kieron O'Hara. Why should i? cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance*, 6:41–48, 6 2018.

[16] Kimberle Crenshaw. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory, and antiracist politics. *University of Chicago Legal Forum*, 1989, 1989.

[17] Mariolga Reyes Cruz. What if i just cite graciela? working toward decolonizing knowledge through a critical ethnography:. *Qualitative Inquiry*, 14:651–658, 6 2008.

[18] Dana Cuomo. Domestic violence, abolitionism, and the problem of patriarchy, 2020.

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

[20] Cynthia Enloe. *Bananas, Beaches and Bases*. 2019.

[21] Sheena Erete and Jennifer O Burrell. Empowered participation: Exploring how citizens use technology in local governance.

[22] Shon Faye. *The transgender issue : an argument for justice*, volume 1. Penguin Books Ltd, 2021.

[23] K.M. Fierke. Critical theory, security, and emancipation, 11 2017.

[24] 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, 11 2019.

[25] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proc. ACM Hum.-Comput. Interact*, 1, 2017.

[26] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "a stalker's paradise": How intimate partner abusers exploit technology. *Conference on Human Factors in Computing Systems - Proceedings*, 2018-April, 4 2018.

[27] Bev Gatenby and Maria Humphries. Feminist participatory action research. *Women's Studies International Forum*, 23, 1 2000.

[28] Glitch. The ripple effect: Covid-19 and the epidemic of online abuse. 2020.

[29] Kishonna L. Gray. Intersecting oppressions and online communities: Examining the experiences of women of color in xbox live. *Information Communication and Society*, 15, 2012.

[30] Xavier L. Guadalupe-Diaz and Jana Jasinski. "i wasn't a priority, i wasn't a victim": Challenges in help seeking for transgender survivors of intimate partner violence. *http://dx.doi.org/10.1177/1077801216650288*, 23:772–792, 6 2016.

[31] Hacking//Hustling. Posting into the void: Studying the impact of shadowbanning on sex workers and activists.

[32] Lucy Hackworth. Limitations of "just gender": The need for an intersectional reframing of online harassment discourse and research. *Mediating Misogyny*, pages 51–70, 2018.

[33] Bridget A Harris and Delanie Woodlock. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, 59:530–550, 4 2019.

[34] Sam Havron, Diana Freed, Rahul Chatterjee, Damon Mccoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. *Proceedings of the 28th USENIX Security Symposium*, 2019.

[35] Virginia Held. Can the ethics of care handle violence? *Ethics and Social Welfare*, 4, 2010.

[36] Nicola Henry, Asher Flynn, and Anastasia Powell. Technology-facilitated domestic and sexual violence: A review. *Violence Against Women*, 26, 12 2020.

[37] Helen Hester. Care under capitalism: The crisis of "women's work". *IPPR Progressive Review*, 24, 2018.

[38] Arlie Russell Hochschild. Global care chains and emotional surplus value, 2015.

[39] Hera Hussain. Trauma-informed design: understanding trauma and healing, 2021.

[40] Kathrin Hörschelmann and Elisabeth Reich. Entangled (in)securities: Sketching the scope of geosocial approaches for understanding "webs of (in)security"1. *http://dx.doi.org/10.1080/14650045.2016.1214821*, 22:73–90, 1 2016.

[41] Mariame Kaba. Free us all – the new inquiry, 2017.

[42] Thomas Kadri. Networks of empathy. *Utah Law Review*, 2020:6, 7 2020.

[43] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. *DIS 2019 - Proceedings of the 2019 ACM Designing Interactive Systems Conference*, pages 527–539, 6 2019.

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

[45] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 'internet of things': How abuse is getting smarter. *SSRN Electronic Journal*, 3 2019.

[46] Audre Lorde. A burst of light. *Essence*, 18, 1988.

[47] Vanessa A. Massaro and Jill Williams. Feminist geopolitics. *Geography Compass*, 7:567–577, 8 2013.

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

[49] Christine E. Murray, G. Evette Horton, Catherine Higgins Johnson, Lori Notestine, Bethany Garr, Allison Marsh Pow, Paulina Flasch, and Elizabeth Doom. Domestic violence service providers' perceptions of safety planning: a focus group study. *Journal of Family Violence*, 30, 4 2015.

[50] Mark Neocleous. *Critique of security*. 2003.

[51] Lesley Nuttall, Jessica Evans, Miriam Franklin, Sarah Burne, James Designer, and Amy Magistris. Coercive control resistant design. 2019.

[52] 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. *ACM International Conference Proceeding Series*, pages 1–15, 9 2019.

[53] Eva PenzeyMoog. *Design for Safety*. A Book Apart, 2021.

[54] Deborah Powney and Nicola Graham-Kevan. Male victims of intimate partner violence: A challenge to the gendered paradigm. *The Palgrave Handbook of Male Psychology and Mental Health*, pages 123–143, 2019.

[55] Nithya Sambasivan, Tara Matthews, Amna Batool, Kurt Thomas, Nova Ahmed, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. "they don't leave us alone anywhere we go": Gender and digital abuse in south asia. *Conference on Human Factors in Computing Systems - Proceedings*, 5 2019.

[56] Laura J. Shepherd. The state of feminist security studies: Continuing the conversation. *International Studies Perspectives*, 14, 2013.

[57] Julia Slupska. Safe at home: Towards a feminist critique of cybersecurity, 2019.

[58] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. *Conference on Human Factors in Computing Systems - Proceedings*, 5 2021.

[59] Julia Slupska and Leonie Maria Tanczer. Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things, 6 2021.

[60] Natalie J. Sokoloff and Ida Dupont. Domestic violence at the intersections of race, class, and gender. *Violence Against Women*, 11, 1 2005.

[61] Bernd Carsten Stahl, Neil F. Doherty, Mark Shaw, and Helge Janicke. Critical theory as an approach to the ethics of information security. *Science and Engineering Ethics*, 20, 2014.

[62] Evan Stark and Marianne Hester. Coercive control: Update and review:. *Violence Against Women*, 25:81–104, 12 2018.

[63] Lisa Sugiura and April Smith. Victim blaming, responsibilization and resilience in online sexual abuse and harassment. *Victimology*, pages 45–79, 2020.

[64] Sharifa Sultana, Mitrasree Deb, Bhattacharjee Ananya, S. M.Raihanul Alam, Shaid Hasan, Trishna Chakraborty, Prianka Roy, Samira Fairuz Ahmed, Aparna Moitra, M. Ashraful Amin, A. K.M.Najmul Islam, and Syed Ishtiaque Ahmed. Unmochon': A tool to combat online sexual harassment over facebook messenger. *Conference on Human Factors in Computing Systems - Proceedings*, 5 2021.

[65] 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*, 9 2021.

[66] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. Sok: Hate, harassment, and the changing landscape of online abuse. *2021 IEEE Symposium on Security and Privacy (SP)*, pages 247–267, 5 2021.

[67] J. Ann Tickner. Feminist responses to international security studies. *Peace Review*, 16, 2004.

[68] Clinic to End Tech Abuse. Ceta | resources.

[69] Joan C. Tronto. *Moral Boundaries*. Routledge, 1993.

[70] 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. *Proceedings of the 29th USENIX Security Symposium*, pages 1893–1909, 5 2020.

[71] 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. ACM, 5 2021.

[72] Victoria Turk. Covid-19 has made ending online abuse even more urgent | wired uk.

[73] Tech vs Abuse. How can tech help address abuse?, 2019.

[74] Benjamin Wittes, Cody Poplin, Quinta Jurecic, and Clara Spera. Sextortion: Cybersecurity, teenagers, and remote sexual assault, 2016.

[75] 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*. 2021.

7 Appendices

7.1 Appendix 1: List of participants

Participants and their organisations are listed in Table 1. As we are promoting advocates as experts in their field, we wanted to give advocates the chance to be identified by their name and organisation should they choose to do so [17]. Consequently, although participants in the study are pseudonymous by default, participants could also opt-in to use their real name. Asterisks (*) indicate areas where participants chose to use a pseudonym or keep details confidential.

7.2 Appendix 2: Interview protocol

1. Can you describe your role?
2. How did you first become involved in addressing the problem of technology-facilitated abuse (or 'tech abuse'?)
3. What kinds of tech abuse do you see most frequently?
4. How do you support survivors to address tech abuse? you walk me through a case that you thought was particularly important or interesting?
5. (If psychological security has not come up) How do you address psychological distress which arise as a result of tech abuse in your work?
6. What challenges do you face in supporting survivors?
7. Are there any demographic factors (like gender, race or immigration status) particular to the victims you support that shape their experience of tech abuse?
8. What kinds of mistakes can advocates make when supporting survivors of tech abuse?
9. Did you receive any formal training in supporting victim-survivors of tech abuse?
10. How does providing this support affect you?
11. What problems have you identified in the design of these technologies?
12. What would you want to say to companies that produce and sell digital technologies?
13. Is there anything else I should know about? Anything else you wanted to tell me?

Name	Organisation	Role	Focus	Location
Natalie Dolci [3]	Safe Campus and Technology-Enabled Coercive Control Initiative	Senior Violence Prevention and Response Specialist	Campus violence prevention and tech enabled coercive control	USA
Stephanie*	*	*	Domestic violence	*
Toby Shulruff	*	*	Domestic violence	USA
Sarah	*	*	Family violence	*
Luiza*	*	*	Women's services	*
Spike Curtis	Technology-Enabled Coercive Control Initiative	Volunteer technologist	Technology-enabled abuse	USA
Adam Dodge	End Technology-Enabled Abuse	CEO	Technology-enabled abuse	USA
Chris Warner	Technology-Enabled Coercive Control Initiative	Volunteer technologist	Technology-enabled abuse	USA
Susan Hickey	Harris County Domestic Violence Coordinating Council	Advocacy Specialist	Domestic violence	USA
Rayme Lacey	Heart of Grant County	Advocate	Domestic violence	USA
Matthew*	*	Advocate	Domestic violence	*
Ben Walker	Technology-Enabled Coercive Control Initiative	Volunteer technologist	Technology-enabled coercive control	USA
Rebecca*	*	*	Sexual violence	*
Anastasia*	*	*	Domestic and sexual violence	*
Amy Jacques	*	*	Domestic violence	*
Metzli Mejia	LA LGBT Center	Legal client advocate	LGBT+ rights	USA
Hera Hussein	Chayn	Founder & CEO	Gender-based violence	Global
Eva Galperin	Electronic Frontier Foundation	Director of Cybersecurity	Digital privacy & civil rights	USA
Bridgette Alexander	*	Domestic Violence Educational Specialist	Domestic violence	USA
Seabata Makoae	She-Hive Association and MenEngage Network Lesotho	Social worker and coordinator	Gender activism	Lesotho
Milcah*	*	Attorney	*	South Africa
Emma Pickering	Refuge	Tech Abuse Team Manager	Domestic violence	UK
Sol*	*	*	*	*
Farah Sattar	DCRYPTD	Founder and Security Researcher	Digital security	USA
Kate Worthington	Revenge Porn Helpline	Senior Helpline Practitioner	Intimate image abuse	UK

Table 1: Participant list