Abusive Partner Perspectives on Technology Abuse: Implications for Community-based Violence Prevention

ROSANNA BELLINI, Cornell University, USA

Inaccurate assumptions about people who abuse technology known as 'tech abuse' can inhibit effective socio-technical interventions for at-risk populations, including survivors of intimate partner violence. Our study aims to rectify this oversight through a synthesis of seven research projects on how 152 abusive partners (APs) discuss and understand their malicious use of technology in face-to-face interactions. AP accounts about tech abuse are rich sources of insight into tech abuse, but demonstrate a heterogeneity of awareness of, choice to use, and ability to desist from participating in tech abuse. To ensure immediate practical benefits for practitioner communities, we also engaged 20 facilitators of abusive partner intervention programs (APIPs) in focused group discussions to identify potential solutions for addressing tech abuse in their programming. Findings reveal that facilitators grapple with a complex set of challenges, stemming from the concern about teaching APs new abusive techniques in-session, and lacking professional tools to investigate, evaluate, and resolve tech abuse attacks. Our work concludes with valuable insights into addressing tech abuse in the APIP ecosystem, and offer targeted lessons for the CSCW community and stakeholders in violence prevention.

CCS Concepts: • **Human-centered computing** → *Empirical studies in collaborative and social computing.*

Additional Key Words and Phrases: intimate partner violence, domestic abuse, abusive partner, technology-enabled abuse

ACM Reference Format:
Rosanna Bellini. 2024. Abusive Partner Perspectives on Technology Abuse: Implications for Community-based Violence Prevention. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 15 (April 2024), 25 pages. https://doi.org/10.1145/3637292

1 INTRODUCTION

Intimate partner violence (IPV) is a mainstream criminal justice, moral, social and health issue worldwide. The misuse of digital technologies ('tech abuse'), a common feature of most reported cases of IPV [25, 39], provide an abusive partner (AP) with new ways to coerce, control, harass, and intimidate a current or former partner. Studies with survivors have shown that APs manipulate readily-available technologies to track and monitor their location [85], read their private messages [30], and expose private and sensitive information online to publicly humiliate them [31]. While CSCW scholars have welcomed a holistic response understanding those who use abusive behaviors [4, 10, 51], and the interventions that support them [26, 29], work is still scant on understanding the people who use tech abuse; abusive partners.

Simplistic views of 'bad actors' can reinforce unequal power dynamics [12, 13] by pushing developers to rely on generic anti-abuse strategies [32, 83], putting vulnerable groups at further risk of abuse. As Freed et al. [32] identify, simply improving privacy controls to block APs on social media or phones, does not prevent their abuse, and may even escalate the risk of harm from online

Author's address: Rosanna Bellini, Cornell University, New York, NY, USA.

ACM 2573-0142/2024/4-ART15
https://doi.org/10.1145/3637292

harassment to physical violence. Other anti-abuse mechanisms such as anti-phishing or fraud prevention, are also designed with predominantly financially-motivated adversaries in mind [83], which can overlook the complex social goals of an AP set on coercion and control [3]. It is thus imperative to gain an accurate understanding of technology abusers, their explanations for their actions, and the challenges that interventions that address APs face in responding to disclosures of tech abuse to promote digital safety for all. [6].

Abusive partner intervention programs (APIPs) play a *"symbolically significant"* role to address the wider societal problem of IPV by focusing on those responsible for harms [93]. By working in tandem with other local community services, APIPs offer support to APs who have perpetrated violence in intimate relationships, helping them develop responsibility for their actions, and cultivate the drive to change their complex patterns of abuse [8, 10]. Although prior work have explored the challenges faced by frontline workers in addressing tech abuse, these have exclusively been focused on survivor-facing care [32, 76, 98]. As effective work to mitigate abuse necessitates safe and effective work with survivors and APs [96], stakeholders must have the confidence to challenge and change harmful behavior at its source. As APIPs can act as vital cornerstones for APs to reflect on their use of harmful behavior, such insights can also inform the growing number of digital tools that equip APs with the means to pursue non-abusive behaviors and relationships [35, 37, 96].

We address these pressing concerns by contributing the most in-depth qualitative study to date that examines the nature and response to disclosures of participation in tech abuse attacks in APIP settings across the United States (US), the United Kingdom (UK) and Australia. Through a comparative analysis [77] of the data of seven qualitative studies, pertaining to 152 APs and 68 APIP facilitators, we examine how disclosures of tech abuse by APs themselves are processed across 61 individual APIP sessions. Using a blend of discursive psychology and critical approaches to discourse analysis we offer the first insight into how APs recognize, rationalize, and desist from using technology to harm survivors.

The discoveries from this analysis are multiple. We identified that APs were likely to confess to destroying a survivor's device, sending harassing or threatening messages, and engaging in non-consensual intimate surveillance. These forms of abuse were considered by other APs to be socially acceptable and condoned, despite the various technical attacks that are known in this context [31, 38, 72, 85, 97]. While many APs argued that such actions were in response to acting in the heat of the moment or to safeguard a survivor from further harm, many APs shared bespoke strategies for resisting the urge from further participating in further attacks.

In response to these disclosures of perpetration of tech abuse, we identify that APIP facilitators face many complex barriers when working with APs. At the point of referral, APIP practitioners are often left without sufficient information to grasp the extent of technology abusive behaviors by an AP in their care. These challenges then ripple into being unable to establish groundtruth in disclosures cases of tech abuse in-session, and fear that any disclosure could lead to facilitating spaces of adversarial learning or feedback to other APIP attendees.

In summary, this work makes several contributions to the computer-supported cooperative work (CSCW), Human-computer interaction (HCI), and Computer Security (CS) literature:

(1) We contribute the most comprehensive study to date into AP's awareness of, disclosures of use of, and desistance from using tech abuse.
(2) We provide a chronological map that showcases the intricate challenges APIP professionals encounter when addressing tech abuse.
(3) We suggest practical measures for both APIP contexts and wider research communities to effectively address tech abuse in interventions with APs.

2 BACKGROUND AND RELATED WORK

Intimate partner violence (IPV) describes a pattern of controlling, coercive, or threatening behaviour, violence or abuse between current or former intimate partners [18]. IPV can consist of psychological, physical, sexual, economic, and emotional forms of abusive behaviour [17, 79, 82], all of which digital technologies have been well-documented to extend and exacerbate [3, 30, 31, 55]. As such, technology-facilitated abuse ('tech abuse' hereafter) — though inevitably hard to measure — is estimated to be inherent in most reported cases of IPV [38, 93, 97]. While tech abuse lacks a standardized definition, in this work, we define it as any intentional behaviors by an individual to use digital technologies to stalk, coerce, intimidate, threaten or otherwise harm a current or former intimate partner. In this work, we refer to people who use abusive behaviors as *abusive partners* (APs), and people who are subject to them as *survivors* to retain the direction of causation [49, 50].

Mitigating tech abuse in IPV contexts. Digital technologies provide an AP with a *"constellation of new tactics"* [68] which erode both temporal and spatial barriers to continuously harm a survivor, even well after a relationship has ended [97, 99]. Prior work has documented how APs benefit from the increased availability of devices [31], the easy access of step-by-step guidance on executing technological attacks [6, 85], and inadequately designed defence mechanisms that fail to anticipate the IPV intimate threat model [3, 31, 52, 74, 75] to conduct such harms. Even small design decisions can have a large impact. For example, while many account owner privileges have been shown to be abused by APs [31], a user who installs, creates or owns an account is still provided an *"outsized role"* in comparison to secondary users [36, 70]. The emergence of social virtual reality [33] and the proliferation of internet-connected products (e.g., internet of things devices [21, 88]) are seemingly creating countless new avenues for APs to exploit.

Many advocates and practitioners have developed technical and non-technical approaches to stem the spread of tech abuse in spite of its significant complexities. We characterize the range of such responses as being: a) *technology-based*, b) *technologically-augmented*, or c) *non-technical but relating to tech abuse*. As an example of a solely technology-based approach, stopNCII prevents non-consensual intimate images from being shared online by detecting and removing them. The *Clinic to End Tech Abuse* (CETA) [30, 32, 86, 87], the *Madison Tech Clinic*, and the *Technology-Enabled Coercive Control Clinic* (TECC) [25] are technology-augmented approaches as such initiatives work directly with IPV survivors to provide tailored advice regarding their privacy and security through video-conferencing [86], and diagnostic tools [30]. Non-technical approaches that have tech abuse as a primary focus can cover safety guides [76], and in-person legal advice on collating digital evidence of harm [53].

In this work, we focus on the latter category of non-technical approaches pertaining tech abuse by focusing on APIP contexts. We do so as this category entails our discoveries can be directly scalable to any organization working directly with APs without the need for understanding novel technical systems (e.g., video-conferencing [8]), including primary care systems, housing, law enforcement, and child welfare. By focusing on the broader in-person context where tech abuse is directly discussed by the people using abuse [39, 89], we may also gain further insight into the motivation, experience, and the perceived consequences that APs have of their actions.

Abuse partner intervention programs (APIPs). APIPs, known as Domestic Violence Perpetrator Programmes (DVPPs) in the United Kingdom (UK) and Australia, or Batterers Intervention Programmes (BIPs) in the United States (US) are community-based interventions directly focused on the accountability of an AP to reform their use of violence. APIPs provide opportunities for APs to engage in *"respectful retribution"*, such as learning and demonstrating non-controlling, non-coercive, and nonviolent behavior [28]. This is achieved by working with an AP through

a case management approach to help them understand how and why abusive behaviors occur. While each APIP is unique, a case may consist of four high-level processes; a referral of a AP from an external organization (e.g., social care, self-referral), an evaluation of the AP's risk profile, an engaged intervention of behavior change, then, the long-term maintenance of sustained support. Each APIP behavior change intervention may last for approximately two hours, in a group setting of eight – twelve attendees APs [63], across 26 sessions, delivered over the course of approximately 29 weeks. The program materials used by APIPs are directly informed by IPV survivors' accounts of abuse, which challenge damaging myths about why IPV has occurred (e.g., victim-blaming, substance abuse). While the unique makeup of a single APIP may vary, many programs have common modules that promote spaces for discussion, shared knowledge, and peer support [69]. All interactions between APs are overseen by highly trained, specialized facilitators who are experts in the interpersonal dynamics of risk and abuse [61, 62].

The lack of availability of specialized workers, lack of funding, and a constant need to demonstrate reductive measurements of success [94] — similar to other voluntary contexts covered in CSCW [1, 14, 80] — are limitations that pose significant challenge to running such programs [8]. One emergent tension in recent years is to *how* to incorporate digital technologies into the syllabus and methods of delivery [10], particularly in light of the growing breadth of research that describes tech abuse [6, 31, 32, 85, 97, 98]. Scholars are particularly divided on how to approach tech abuse with APs. It is debated whether it should be considered a separate form of harm [83], a subset of other coercive behaviors [39], or a combination of the two [25]. To accompany these disputes, practitioners have cautioned the risk of knowledgeable APs teaching each other new forms of abuse. After all, the existence of a supportive online community that actively condones or encourages communities of abuse can also escalate the severity of tech abuse [6, 85, 91]. While fears of collusion may be understandable warranted, others have posited this mirrors more general fears of APIPs — that collecting abusers together in a single location will automatically increase risk — though no studies have shown this to be the case [37]. APIP providers have nevertheless been encouraged to engage with areas of oversight in their syllabus, explore novel counselling approaches, and address harm to protect survivors [59, 60].

3 METHODOLOGY

In this section, we describe our approach to conducting an individualizing, then universalizing comparative analyses (Section 3.1), our study selection criteria and overview (Section 3.2), our identification of tech abuse disclosures (Section 3.3), our approach to data analyses (Section 3.4), and our ethical approach toward analyzing APs accounts (Section 3.5).

3.1 Comparative analysis

In this work, we conduct a novel *comparative analysis* of seven qualitative research projects (Table 2), each performed in-person with APs and skilled APIP professional facilitators (*practitioners* from hereafter) [77]. Comparative analyses can help scholars to build on, rather than inadvertently replicate, existing knowledge [58]. In comparative analysis, two or more processes, documents, data sets or other objects are compared to determine individualizing, universalizing, variation-finding, and encompassing factors [84]. For this work, we chose to use two of the four primary ways of performing a comparative analysis — *individualizing* and *universalizing*. *Individualizing* analyses necessitate an in-depth analysis of multiple works to identify the specific similarities and differences of each study [84]. Conversely, *universalising* analyses explores if a single or set of factors can apply to all cases within a small, selective subset of studies, but not to all cases in existence (i.e., generalizable) [64].

High-Level Study Category	ID	Study Description	AP	P	Research Method(s) Used
Observational studies of existing APIP practices with digital technologies	A	Multi-site observational study to explore areas digital technologies can assist APIP providers with their work with APs [10]	40	6	Focused Ethnography, Participant Observation, and Interviews
	B	Feasibility study on the suitability of video-conferencing software as a method for APIP delivery [7]	6	4	Virtual Observations, Interviews
Design and deployment of digital technologies for in-person activities in APIPs	C	Exploratory study with three APIP providers to design a digital educative tool to be used in-between APIP sessions with APs [8]	32	22	Focused Group Discussions, and Interviews
	D	Digital system for APs to assist learning and build capacity for decision-making in-session [4]	27	4	Design Workshops, Interviews, System Trial and Post-Trial Evaluation
	E	Observatory study across three study sites to investigate the potential for a biophysical tool for APs to navigate social contexts [11]	14	6	Interviews, and Focused Group Discussions
Design and deployment of digital technologies for evaluation and post-APIP activities	F	Digital craft-based activities with APs to facilitate moderated asynchronous peer-support network creation post-APIP [9]	18	6	Design Workshops, System Trial, and Post-Trial Evaluation
	G	Deployment of a voice-based audio tool to measure levels of AP engagement and attitude change post-APIP [5]	15	20	Design Workshops, Participant Observation, and System Trial
			152	68	

Tabela 1. Overview of seven qualitative studies selected for cross-comparison, each displaying a study reference ID (A – G) [4, 5, 7–11], an abstract broad study category description, and a high-level study description. We also denote how many abusive partners (AP) and practitioners (P) were participants in each study, and the research methods selected for each context. All studies took place between 2018 and 2021.

Comparative approaches are especially useful to provide new conceptual, methodological, and empirical contributions to areas that may have been overlooked or otherwise difficult to assert without the compilation of several studies. For instance, in their comparison of three case studies Burgess et al.'s [16] argue their conceptual contribution of *care frictions* (non-compliant patient behavior) could not have been derived from a single study. In addition, Soden et al.'s [78] emphasize the importance understanding case studies in a historical context which may only be possible through contrasting their overarching narratives. Our work extends this growing trend of critical retroactive reflections. Such an endeavour, built upon histories of activist practice, helps to notice *"underlying patterns and relationships"* of abuse that may otherwise go unnoticed [54, 92].

3.2 Study criteria and overview

We selected cases that have similar qualitative traditions, focuses, and study contexts to best represent the original research [66]. Smelser [77] proposes five criteria for selecting units of comparison in comparative analyses, that each should: 1) be suited to the investigator's theoretical problem; 2) be relevant to the phenomenon under study; 3) possess classifying criteria that are empirically invariant; 4) reflect the degree of availability of data to this unit; and 5) showcase decisions to select and classify units should be standardized and repeatable. We used a broad search criteria to elicit APs' firsthand disclosures of tech abuse (broadly defined) by the following criteria:

a. The study's primary focus was on understanding how APs interacted with digital systems and devices through first-hand accounts.
b. All data collection was conducted at field sites that delivered violence prevention programmes (DVPPs, APIPs). Such field sites had to strictly comply with accredited safe practices (i.e., trained professionals, physical safety protocols) to ensure the safety and wellbeing of APs, survivors, their dependents, staff, and the research team.
c. Each study used qualitative, data-driven approaches that promoted the interpretation and exploration of the human experience.

This criteria entailed we excluded numerous qualitative studies on AP behavior of tech abuse from the perspective of survivors, children, practitioners, or other laypersons. While such accounts contain invaluable insight on tech abuse [38, 65], such work often rely on second-hand accounts of intent, thus may inevitably refract the information on AP's firsthand descriptions and reflections on their abusive behavior. At the time of our search, we did not identify a single study whereby

the *abuse* of digital technology by APs of IPV were the primary focus. This reaffirms the novel contribution of this work (Section 1).

To build a corpus of comparative studies, we filtered for studies with data-sharing arrangements (Smelser's [77] 4th requirement). The research team submitted data usage requests to the primary contact of each identified study via email which outlined our study's purpose, data protection strategies, and inquired about ethical approval status. Each research team was also asked to clarify participant consent dimensions for secondary (follow-on) analyses. As our aspiration to design technology to mitigate abuse and improve service user outcomes, this work was aligned with each study's original objectives and fell within the time period permitted (see Section 3.5).

Our pooled dataset were thus drawn from seven independent qualitative studies (A – G) located across the fields of Human-Computer Interaction (HCI), Computer Security, Criminology, and Sociology. Each study worked directly with in-person APs and APIP providers, and were conducted across multiple research sites which span across the UK and the US. This resulted in a total pooled sample size of 152 APs, and 60 APIP professionals, spread across six different APIP programme settings (Table 2).

3.3 Identification of Tech Abuse Disclosures

We collated all qualitative data from Studies A – G and manually reviewed the data to remove primary and secondary identifiers prior to analysis. To organize our data, we used ATLAS.ti desktop offline edition, that was configured to store data locally rather than a cloud. We pooled our data together for a close reading (*familiarization*) of content and gained a feel for each studies' discursive effects across several weeks. As some studies contained image-based data, including photographs of completed design activities from workshops (Studies D, F, and G), the first author extracted any written content on analogue materials into digitized text memo documents. Following sensitization, we then pruned our data to examine the authentic perspectives of APs and APIP facilitators in this work. This meant we only analyzed the qualitative segments of the data that focus directly on the AP in each study. We therefore excluded system log data of any systems in-use (Studies D, F and G), auto-ethnographic notes created by the research team about other service professionals (Study A), and interviews with survivors (Studies C and D). Thus, our preliminary data-set for this work resulted in a library of 2059 pages of media files, composed of digital notes of participant quotes (n=491), transcripts of interviews (n=804), focus group discussions (n=448), design workshops (n=210), and post-system trial textual feedback (n=96).

Following the cleaning, pruning, and digitization of the data, we examined it for references to technology or tech abuse. First, we compiled a keyword search of commonly known terms associated with digital technologies and tech abuse before executing via integrated batch queries to mitigate duplicate returns. We complemented this with an extension of Atlas.ti's in-built localized semantic search to find similar sentence fragments that related to tech abuse. We define a *disclosure of tech abuse* by an AP narrating their active participation in perpetrating a technology-based attack. These attacks were drawn from five taxonomies that encompass all known attacks in IPV contexts, spanning subtypes such as financial [3] and surveillance-based abuse [6, 85], and specific device types like IoT which also extended to general grand names (e.g., Alexa, Echo). As we report in our findings (Section 4.2.1), we discovered that APs frequently mentioned being targeted by such attacks from others. These incidents were recorded and analyzed separately from the rest of our data. Our final working dataset contained 683 files of rich first-hand descriptions of an AP's understanding, or use of tech abuse, and the challenges practitioners encounter while such disclosures occur.

3.3.1 Representative disclosure. Although each work had different research objectives, each study included detailed qualitative descriptions of tech abuse disclosures. Here, we provide a representative interaction using amalgamated quotes for anonymity from several APs to illustrate the discursive nature of APIP sessions:

> **Abusive partner #1:** *"Me and my partner have been fighting for months ... she'd always know which buttons to press to get me started ... she stopped answering my phone calls when I'd check in asking 'where are you?' so instead I started texting her mates, to see where she was. I didn't see anything wrong with it, it's normal to tell your partner where you're going ... I set up the [home surveillance system] so I could get a notification every time she left the house to ... "* (Amalgamated, P6, P29, and P81)
> **APIP facilitator:** *"... Okay, I'm just going to stop you from going any further, as I think you've skipped over something important ... I'd like the you and the group to reflect on why it's important to know where your partner is"*
> **Abusive partner #2:** *"Yeah like … I think the real question is: [AP#1], why do you need to text her all the time? [Are] you bored in an evening?"* (Amalgamated, P2, P39, and P82)

This interaction characterises several elements about the unique nature of APIPs. Firstly, that APIP sessions are dynamic and prioritise learning through discussion between facilitators and APs, and amongst APs themselves. Second, that disclosures of tech abuse were often delivered following the disclosure of another form of abuse. Thirdly, that such disclosures were often interrupted by an APIP facilitator to tactfully mitigate the risk of facilitating APs learning about new strategies for harm — in this case how to set up a home surveillance system for location tracking.

3.4 Discursive data analysis and process

We selected to use a blend of discursive psychology and critical approaches to discourse analysis (as welcomed by prior work in CSCW [19, 48]). The former leveraged the use of psychological concepts such as distancing, introspection, and stigma, which proved invaluable at helping to guide our initial understanding of how APs achieved their self-assigned goals through technology [6, 44, 95]. To complement this, the latter focused specifically on how these discourses were reinforced, reproduced and legitimized which offered valuable guides in critiquing dominant approaches to privacy, security, and safety of at-risk populations [56]. We did this by labelling any discursive strategies used by APs to describe their use of tech abuse, and their negotiation of their subjective positions they chose to speak from (e.g., as a survivor, as a 'changed man'). A combination of both these approaches allowed us to bridge the gap between calls for listening to the *"invisible agents"* of tech abuse [49], while also critically connecting accounts to wider social systems of power.

We chose to conduct our case comparative analysis in two stages using discursive psychology and critical discourse analysis to elicit insights [73]. First, we conducted our *universalising* case comparative analysis on 152 APs disclosures of tech abuse in-person in APIP settings across seven research projects (case study hereafter) (Section 4). This step first enables our analysis to characterize what a typical and atypical disclosure of tech abuse may look like. We hypothesized such findings could serve as a point of reference for our *individualizing* comparative analysis of a single research project consisting of three focused group discussions (FGDs) with 20 APIP professionals. We did this to identify challenges to directly addressing tech abuse disclosures with APs (Section 5).

3.5 Ethical approach and limitations

This work investigates APs who may use linguistic techniques to avoid, minimize, and otherwise deny their participation in abusive acts [6, 34, 44, 47]. While our research focuses on APs, we do so to contribute toward building safer lives for present, and potential survivors of IPV. We used

ID	Study description pertaining to tech (ab)use
A	Study on the use of digital technologies by a Northern England organization to support 40 APs in their 12-month journey toward non-violence. Such services included one-on-one support, counseling, APIP programs, and creative arts practice sessions tailored to meet the diverse needs of male APs. The study involved bi-weekly observations of active APIP programs with 8—10 APs, as well as discussions and interviews with APs and practitioners to investigate how digital technologies played a role in redistributing responsibility for violence prevention. APs engaged in a range of conversations, yet prominent ones reflect the changing role of technology in their lives, the use of helpful online resources, and participation in abusive behaviors post-separation.
B	A mixed methods study that explored the challenges and opportunities of the first live online program for six court-mandated APs in the North East of the US. APs participated in an intake interview, 27 weekly 90-minute group sessions, and an exit interview. The data collected included 40 hours of observation (25 sessions), interviews with program facilitators and observers, and six enrolled APs. Participants explored the viability of the online digital program, an AP's engagement in digital activities, and uses of technology for work. The study, as a result of being digital introduced a specific focus on remote uses of technology abuse and APs expressed around privacy related to the online program.
C	Exploratory study on how digital technologies could be used to further support to APs enrolled in APIPs and highly motivated to change behavior. This project used an adapted user-centred design (UCD) approach on researching potential design opportunities for a digital platform to increase an AP's engagement in the APIP content. This work consisted of a series of focus groups with 26 APs enrolled in three APIP contexts and 20 as APIP practitioners across three research sites across England, UK. Discussions of tech abuse played a strong role in this work where APs admitted to using it, particularly in post-separation periods to prolong abuse.
D	Study focused on an evaluation of a two-day educational course for APs, covering the impact of intimate partner violence (IPV) on survivors, health risks associated with IPV, and maintaining healthy relationships. The study included participant observations, preliminary interviews with APIP facilitators, and a design workshop for a technical aid that could help with making decisions about non-abusive actions. A web and mobile system for 27 APs was trialled to highlight challenges in technology engagement, and the importance of an APs' agency in supporting non-violent behaviors. APs were asked to reflect on their agency, choice and decision-making skills with respect to using digital technologies for harm.
E	Exploratory study on the use of communication tools at a research site to engage 14 APs in voluntary enrollment for APIPs. This APIP consisted of weekly two-and-a-half-hour sessions for 25 weeks, with an additional 12-month relapse prevention program. Groups of APs were asked questions on technology use, calming down, and promoting non-violence, with each activity lasting 30–40 minutes. The study elicited several lengthy disclosures of the use of tech abuse towards current partners by APs which were often combined with emotional, physical, sexual, and financial abuse.
F	Study focused on a moderated peer-support network for APIPs across three research sites, considering the network's effectiveness in sustaining long-term APIP engagement. The study spanned ten months and involved five design workshops, the deployment of a new digital system with 18 APs, and a structured evaluation of their system usage. APs were asked about their initial peer-support methods and the role of technology in facilitating the network beyond the APIP. Questions were asked to investigate the supporters and barriers to behavior change after completing an APIP, with a specific focus on technology use after the program.
G	An investigative study of a voice-based technology to gather and utilize feedback for evaluating an APIP. The study spanned four months, including ethnographic observations of four deployments with eight APs and reflective discussions with four APIP facilitators. The intervention involved interactive sessions where attendees, facilitators, and the lead researcher could engage in dialogue using prompts, educational materials, and videos. APs and APIP professionals were asked to reflect on the potential of voice-based technologies for reflecting on and improving service practices, as well as its practical role in broader service design.

Tabela 2. Textual description of seven qualitative studies (Study A — G) identified for comparative analysis.

critical and discursive analytical approaches that do not take what APs describe at face value. As any ethical work with APs has to center the survivor's needs and aspirations, we chose to only analyse work with APIP professionals and Integrated Safety Support (ISS) workers who work with survivors. All data were collected in contexts that abide by safety-focused standards that hold APs accountable for their abusive behaviors [81].

All studies included in this analysis gained full ethical approval from the Research Ethics Committees (RECs) at their relative institutions. All APs and APIP professionals consented to use of their data for research to improve intervention and technology design and thereby enhance service user outcomes. Such consent processes also covered analysis of redacted participant data for up to five years following the publication of the primary studies. In each study, participants were informed that their participation, non-participation, or withdrawal would not impact the quality of support services they received. Furthermore, no financial incentives were provided to encourage participation. Participants were also advised about the limitations of research confidentiality which included any potential risks to the survivor, their dependents (i.e., children), or themselves.

All members of the authorship team have extensive experience in IPV and related research contexts, and are trained in safeguarding vulnerable research participants. As IPV can be an emotive topic [22, 57, 90], each author has a self-care plan for mitigating vicarious trauma and

burnout. While the physical risk of violence by APs to researchers is rare [23, 41], the risk of *collusion* with APs — cooperation with an AP to cause further harm to survivors — is far more acute [23, 24]. We thus considered how our work might help adversarial readers learn ways to harm survivors [12]. APs could also read our discoveries regarding the challenges faced by many practitioners and deepen these wedges by undermining the integrity of APIP. We thus omit the names of hardware and software tools, and step-by-step instructions that could make replicating these instances possible. We also requested that two experts in privacy and security and two representatives from the APIP providers review our work for this risk. Both sets agreed such attacks were already widely known, and our implications for improvements would be immediately beneficial to practitioners.

3.5.1 Limitations. All disclosures of technology abuse are self-reported and retrospective meaning some APs may have only understood their actions as abuse after discussing them. Social desirability reporting — the tendency for participants to present themselves in a generally favorable fashion — is also a common risk for all studies with APs [6, 43, 92]. However, such reporting biases help to provide insight into how APs discuss technology abuse in social settings.

Each study included in this work contained ample in-depth disclosures of participation in technology abuse against survivors. Nevertheless, each study was not primarily designed to identify, address, and characterise these disclosures. As such, our data may have revealed more insightful and focused revelations about technology abuse through a focused study design.

Finally, all of our studies under review took place in the UK, US, and Australia meaning that the researchers, practitioners, and APs in this study all were all based in the Global North. Although this is representative of the higher concentration of APIPs in Western countries globally [2, 37], we are interested in expanding this work to encompass future internationally inclusive contexts.

4 DISCLOSURES OF TECH ABUSE PERPETRATION

Despite previous theories suggesting that face-to-face interactions between APs would hinder tech abuse disclosures [6, 92], all APs in our sample extensively discussed using technology to abuse their current or former partners. As such accounts were rich in detail, we were able to clarify what types of tech abuse were disclosed, when these attacks took place, and where in the APIP these were shared with other APs (Section 4.1). We then situate these disclosures in the wider APIP social context, by commenting on an AP's awareness of, justifications for participation in attacks, and strategies for desistance (i.e., resisting using tech abuse) (Section 4.2).

4.1 Technical attacks

In this section, we take a closer look at the nature of the tech abuse disclosures in our dataset. While our analysis did not surface new forms of attacks, it did identify more frequently disclosed types of attacks in an APIP environment, the sophistication and range of attacks used, and when these disclosures occurred.

4.1.1 Prevalence. The most prevalent form of tech abuse as reported by APs was that of *sending offensive, hurtful, or threatening messages* to a survivor (n=56). APs shared that this could be performed via a range of different devices, from mobile phones, to instant messages on social media, to online games with communication functionality. Although not all APs described the content of these messages that enabled them to be threatening, each disclosure was paired with a description that included inducing fear, alarm, or distress to a survivor (irrespective of if an AP found this response to be justified). In one case, a facilitator asked a group of five APs to reflect on a time where they had deliberately hurt someone. One AP (AP31, SC) shared a high-level summary of the graphic contents of an SMS message that they had sent an ex-partner, containing threats

to murder them and then dispose of the body. We identify that threats of this nature were often reported to occur at the end of a relationship, or when a survivor had moved out of a shared domestic environment; presumably as access to physical devices were no longer available [55]. Such a finding is also consistent with research highlighting abusive messaging as a continuation of coercive control post-separation, after a survivor has left an abusive relationship [22, 25].

The second most prevalent attack mentioned involved *physically destroying a device*, which was frequently reported by APs (n=43), especially in situations where there was an interpersonal conflict with the survivor and they were in close physical proximity. Such devices included personal smartphones, televisions, tablets, smart speakers, and laptops. When devices like a family tablet were shared, APs recognized that it meant the children's devices were being destroyed.

Finally, short-range and remote *monitoring and surveillance* also featured heavily in each study in our dataset (n=27), with descriptions of installing home security systems for the reported 'protection' of a survivor and their dependents. These could include home security systems, or surveilling a survivor through public-facing websites or apps.

Other forms of tech abuse, such as the distribution of image-based sexual abuse (n=2), private exposure of public information (n=2), and impersonation ('catfishing') (n=1) were infrequently reported in our dataset. In contrast to other forms of tech abuse, we found that APs always expressed embarrassment or shame when making these disclosures.

4.1.2 Proficiency and range of attacks. Despite marking identifiable technical attacks in our analysis, we also identified several statements that APs describe using technology that we judged to be implausible or unlikely. This tendency to boast about specific technical attacks has been noticed in prior work on pro-abuse forum dynamics [6], though, we identify that these boasts were often paired with implausible uses of current technical capabilities. For instance in one APIP session, we identified that an AP boasted about being able to *"control the direction of the Wi-Fi waves"* (AP14, SE) in the home to remotely turn a survivor's devices on or off, but did not provide any low-level details as to how this might be possible (e.g., interference with routers, internet traffic). While APs may deliberately overemphasize their technical skills to scare a survivor, they could also misunderstand the basic functioning of technology through their disclosures. An alternative explanation for this could be that APs wish to be seen as highly proficient by other APs in an APIP setting.

Akin to other types of abuse [24, 43], many APs framed their use of technology abuse as a one-time occurrence that had happened in the past. This claim, however, stood in contrast to the discovery that the APs would admit to multiple forms of tech abuse across multiple APIP sessions. For example, in an earlier session where an AP (AP150, SG) was recounting their relationship with an ex-partner, they shared they had only destroyed their partner's laptop once. However, in a later session, the same AP admitted to destroying multiple laptops and devices multiple times to inconvenience the same ex-partner in their participation in their work. Although this may be explained by the limitation of APs ability to remember said incidents, this could also serve to undermine the survivor's credibility a bystander's ability to recognize the abuse as ongoing and systematic. APs could however be masking the extensive nature of their controlling behaviors by fixating on one form of technological abuse rather than part of a wider pattern of coercive control.

4.2 The social context of tech abuse disclosures

Building on the characterization of the disclosures of tech abuse in APIP settings (Section 4.1), in this section, we discuss the findings of our universalizing comparative analysis. We begin by reporting an APs' *awareness* of tech abuse *as* abusive; their self-identified *justifications* for participating in tech abuse; and strategies for *desisting* from participating in future attacks.

4.2.1 Awareness of, and use of technology abuse. In the first stage of our process for modelling an AP's relationship to tech abuse, we identify it is important to identify the level of awareness APs may have toward the topic. We investigate how APs perceive the concept of tech abuse in an abstract sense, as a bystander or as an individual who admitted to performing specific forms of 'socially acceptable' forms of tech abuse.

A victim or bystander, but never an offender. When the topic of tech abuse emerged organically across APIPs, there was a wide definition of what it meant. Some APs (AP6, 30, 64) suggested that broader uses of technological harm, such as spreading online hate, organizing rallies of networked harassment online (particularly against celebrities), and identity theft constituted an abuse of technology. Although APs were unsure about the exact definitions of tech abuse (as may be expected), several were keen to state that technology abuse was rarely located in an intimate partnership – particularly not their own. For instance, midway through a group APIP session (SD), an APIP facilitator asked an AP to reflect on their use of harassing text messages to intimidate a current partner:

> *"What's going through your mind when you send that text?"* (P24, SD)
> *"I mean ... who hasn't sent nasty texts to a partner before? I mean, I think everyone has haven't they? If they haven't I don't think they're being honest ... Everyone has said something they know they shouldn't have over a text."* (AP21, SD)

For APs that did provide concrete examples of technology abuse between partners, curiously this occurred when reporting personal accounts of friends or family members who had used technology abuse against an intimate partner. APs recounted plenty of anecdotes of friends who had reportedly *"went off on their [partner] on social media"* (AP15, SG) through using multiple, harassing and targeted messages against a partner, particularly at relationship cessation. We suspect that disclosures about other friends of family members occur so frequently, as this enables APs to discuss this form of abuse and express their views. However, it also provides them cover to do so without immediately assigning personal responsibility or agency to it.

Our analysis also discovered it was far more common for an AP to talk about being the *victim* or target of technology abuse than they were to admit to purposefully using it against a survivor. In these situations, APs described at length as to how their current or former partner had used intimate partner surveillance (IPS) to track their location, or check their social media without permission (e.g., shoulder-surfing or account compromise.) Such disclosures seemingly directly contradicted the previous answers offered by the same APs about being unaware of what technology abuse included or how tech abuse could be used to harm in intimate partner contexts. For instance, when a researcher posited the question if an AP had been personally targeted by tech abuse by anyone they knew in a one-on-one session, they replied:

> *"My ex-partner, yeah she cloned my phone ... so every time I was getting a text she was also getting that. She knew exactly where I was, every single day and I didn't know that until we separated and one of her family members told me 'you know that she cloned your phone right?"'* (AP30, SC)

Although we lack the ground truth to this account, we identify that APs consistently framed themselves as the one being subject to technological harms, rather than being the one perpetrating these actions. While some APs could, to some extent, understand how technology abuse was harmful, by citing that they had personally been harmed by it, we found few instances where APs explained how survivors could be hurt by their use of technology abuse.

Socially acceptable forms of technology abuse. When APs did disclose to using technology against a current or former intimate partner, despite the range of identified attack vectors identified

by scholars [31, 97, 99], APs *admitted* to only using three distinctive types of technology abuse: the destruction of a survivor's digital property (e.g., a phone); sending abusive and threatening messages; and, location-tracking via dual-use GPS applications (see Section 4.1). We identified several APs who described situations where they had damaged or permanently broken a survivor's personal devices, such as a smartphone or a tablet, that a survivor had been using at the time. When recounting their stories of abuse, APs were careful to reinforce that they had not physically harmed their partner while doing so; as APs were likely to acknowledge physical violence as abuse. In a recap session at the start of an APIP session, where APs are encouraged to reflect on if, and when, they used harmful behavior over the weekend, an AP shared:

> *"yeah I smashed her phone up once ... [I] threw the thing at a wall and the screen cracked and stuff so it couldn't be used ... I guess the wall also suffered too"* (AP12, SC)

A few APs also mentioned to APIP groups how they had threatened their partners physically by sending text messages and instant messages. It was revealed that one AP sent the threatening text when they knew their ex-partner would see it, specifically so that it wouldn't be missed; *"She gets off for her lunch break at [time] so I know she'll have seen it"* (AP27, SD). As digital devices facilitate digital location tracking through GPS coordinates, many smartphone devices proved to also act as homing beacons for an abuser to narrow down on identifying where a survivor was. For instance, when prompted by a researcher if an intimate partner had ever felt uncomfortable with how they got in contact with them, an AP shared:

> *"yeah I tried to make phone calls to find where my wife was ... "oh right you said you were going to be back [home] an hour ago?" When she didn't answer and hung up ... after that I just put the family on a location sharing app and problem solved.* (AP3, SE)

Here this evidences that APs often knowingly positioned location as a proxy for inferring who their intimate partner was with, and the type of activity their intimate partner was engaged in such as work or for leisure. APs sometimes paired this a discussion on surveillance with describing a set of permissible actions for a survivor. In one example where an AP was asked to expand on why they chose to use a family sharing application, they replied that this left the survivor little room to be able to protest, specifically in case a survivor was to offer an *"alternative account of what they were up to"* (AP33, SA) to an AP.

4.2.2 Justifications to using technology abuse. Following establishing the level of awareness and acknowledgement of tech abuse, we identify that if tech abuse is used (e.g., such as an act outlined in Section 4.1), it must be coupled with a justification as to how it is used. In contrast to the distancing and dissociative accounts (Section 4.2.1), we identified several instances where APs described conscious and deliberate uses of technology abuse against a survivor to achieve specific and discrete goals. Hearn [43] describes this as when an AP accepts some personal responsibility for the cause of the action, yet absolves themselves of blame that they are personally responsible for the situation. These disclosures of the use of technology abuse by APs were coupled with an insistence that they could not be held responsible for their actions.

Emotional states justify abuse. Some APs ascribed technology with directly causing and invoking their abusive behavior — traditionally through making them angry, frustrated, or feel guilty. For one AP, they described becoming taken over by a *"red mist"* (AP13, SE) when they became angry or frustrated with a survivor, and another AP being *"easily provoked into lashing out online"* (AP20, SD), suggesting that they absolved themselves of their actions. We identified jealousy as a powerful justification, which could potentially have led to a meaningful reflection on one's behavior, but APs instead framed the survivor as responsible. As one AP reflected in a one-on-one session

with a researcher when recounting a recent court case involving the mother of his child and the removal of the child from his custody:

> *"I just couldn't take her taking my kid away, I didn't want my son without his dad ... I installed the [tracking] software ... I wasn't really thinking straight but I was jealous"* (AP1, SF)

As APs demonstrate here, descriptions of frustration, anger or jealousy for an AP provided the emotional reasoning that framed their behaviors as acceptable. In contrast to these powerful and instantaneous emotions, however, they often compelled others to delete evidence of such emotional outbursts, or simply deleted it themselves. The actions primarily involved deleting text messages and instant messages containing abusive and threatening content, typically using their own devices:

> *"It's worse because if you say it, it's gone isn't it. If you send it, it's always there. Sending a text message is there until they delete it. If you say it in word, there's no proof. Only mine and her word isn't it?"* (AP32, SC)

In these contexts, we identified that APs consistently framed their actions, particularly when in an angry or aggressive state, as "not as bad" (AP100, SE). Curiously, we identified a noticeable relationship in whether a AP reported feeling bad with when actions could be used as evidence against them. For instance, sending a harassing text messages or a system log of an installed application were paired with rgeret, but only when said actions could be used against them.

Technological control for the survivors' protection. APs in our analysis described being in situations that actively *necessitated* the use of tech abuse against an intimate partner. Tech abuse was sometimes positioned by APs as a strategic choice to minimize the harm that they were, or could be, inflicting on their survivor. When reflecting on a time where they felt like they were getting substantially angrier following a dispute with an ex-partner, an AP disclosed in an APIP group setting:

> *"I could feel myself hotting up so I just got out of there [home] ... yeah the fighting continued over the phone but I just thought, well that's not as bad as smashing plates again is it?"'* (AP14, SG)

Such accounts highlighted how AP could use technology as a method to prevent themselves from becoming physically abusive in-person with their partner. This in some regard echoes how some APs assume that such actions are 'not as bad' as other forms of abuse. While this could be a potential tactic for APs to minimize the risk of the immediate on-set of physical harm in some situations, survivors still have to choose between different forms of abuse. A desire to 'protect' others through the use of tech abuse could also extend to other members of a family unit, such as children. For instance, upon reading a newspaper article, an AP disclosed concern around the risk of grooming by online sex offenders to his children, and thus disallowed them from social media. They then extended this behavior to his partner:

> *"I didn't let the kids go on social media sites ... like I told them who you can't be connected with on social media, who you can follow and stuff ... it's just not safe out there. Yeah, it's just not safe for her either. You gotta protect your family."* (AP1, SE)

AP who used this excuse could therefore frame themselves as protectors and providers of safety for their family, from external threats and all of the so-called *"nasty people online"* (AP21, SD). In these disclosures, APs framed their actions in a positive light, and the survivor was either *"ungrateful ... dismissive"* (AP2, SD) of such care if they protested. Such narratives are commonplace amongst works that discuss parent-child tracking and negotiation of online safety [20, 45]; yet such messaging could also be informing APs on how to control online activity of adults.

4.2.3 Desisting and reforming abusive behaviours with technology. Finally, for APs who are both aware of, and have actively used tech abuse, we identify many would stress that they were not doing so any more. APs described accounts where some level of acceptance of responsibility and blame was present [43], sometimes involving acknowledgement, disclosure and the admission of fault in how they were using technology. However, many focused on how they were now a reformed individual, yet still struggled with the temptation to use digital technologies to cause harm. Such a duality resonates what other scholars have also termed as a *'double self'* – a violent self who has committed violence and a presenting talking self who is non-violent [34, 44].

A past, digital, destructive self. Many APs, shared that it was hard to concretely define what 'success' from misusing technology in this task entailed. Some accounts described feeling split between whether to *"entirely give up tech"* (AP18, SC) or just *"do it less"* (AP9, SA). When some APs had admitted to using technology to harm others, rather than appeal to physical distancing messages, such as claiming they were entirely without digital devices, we identified another psychological manifestation of distance – past identity. We identified that APs would consistently refer to past actions with digital technologies as those performed by a dark version of themselves, or, a *digital double self* who was described as destructive, easily provoked (resonating, perhaps with [51]), and uncontrollable. This self, that was most often used to describe violent acts, seemingly existed only online (AP18, 56, 110) or, more commonly, when attached to the phone (AP10, 15, 50, 64, 90). When explaining their journey of behavior change to a researcher across the previous three years to a researcher, an AP shared:

> *"I'm a different person now, here, than the man I am online ... I get braver over text, much braver ... I say more in a text than I ever do in person ... yeah it didn't feel like me doing those things."* (AP37, SA)

While such a phenomenon could be reasonably explained by the *online disinhibition effect* – the lack of constraint an individual may feel when communicating online – many APs stated that using communication technologies turned them into an entirely separate, unrecognizable person. For instance, an AP reflects back on his previously abusive behavior towards his children which included a range of different harmful uses of technologies, including sending harassing emails and text messages to them in the past:

> *"I don't recognize that person and what he did ... I look at the messages now and think I don't think I could have written that out as I did"* (AP5, SE).

A reformed individual. In contrast, to a *destructive, digital self*, many APs were keen to establish that the person in the APIP sessions now was different from their digital counterpart. APs often went to significant lengths to describe how they were now rational and thoughtful in their actions with technology; such as using technologies to only organize child-minding duties, and leaving toxic online communities. APs who described themselves in this manner seemingly did not want to deny their abusive behaviors; if anything presented a past self in a self-deprecating and negative light to provide a critical contrast to their present self. In one case, an AP who participated in a group discussion with several researchers shared that he had posted a non-consensual intimate image of a partner online that was later used in court:

> *"I knew it was wrong, but I didn't know it was that wrong until I came here ... if someone told me that I did that all those years ago, obviously it bites you back and it just ain't worth it"* (AP31, SC)

Similarly, APs presented a morally refined self who underwent a transformative learning process, describing the process as *"healing ... what was wrong before"* (AP7, SE). APs shared several narratives

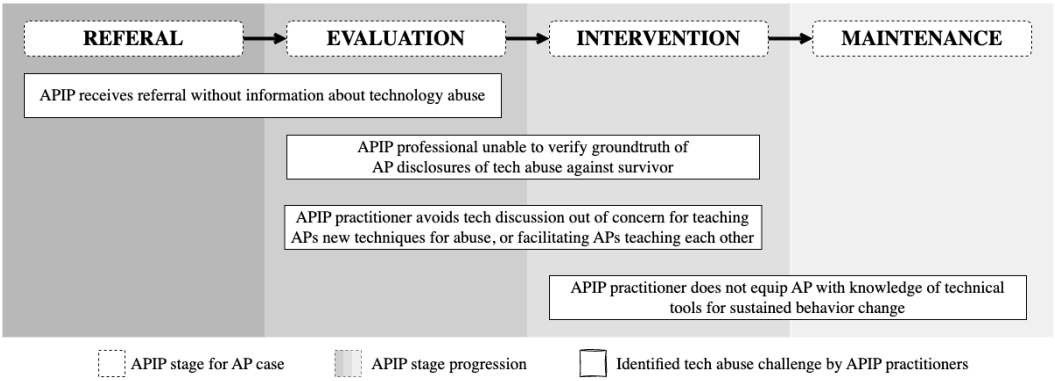

Fig. 1. Four stage diagram that shows the high-level process of a single AP case through an APIP service. We map each significant tension identified to one or more of these key phases to demonstrate the pervasiveness of the problem of addressing tech abuse in an APIP.

that were able to communicate the noble struggle that they had performed to be able to achieve not using technology to harm. For instance, some APs made the association between substance misuse, addiction and dependency to their tendency to maliciously use technologies, being frequently tempted by its close proximity and availability. In some extreme cases, these coping measures resulted in quitting technology altogether, or going 'off-grid'. In a group session on health and wellbeing toward the end of their APIP session with six other APs, one AP disclosed:

> *"the phone is just there ... I could just use it if I wanted to ... I think about doing it often, contacting her when I shouldn't and I see other people contacting their loved ones. Yeah ... it's hard"* (AP12, SF)

5 BARRIERS TO ADDRESSING TECH ABUSE DISCLOSURES IN APIPS

Our characterization of what a typical disclosure of tech abuse looks like (Section 4.1), and trends over time of how they are presented in light of the social environment of APIPs (Section 4.2) help to document a previously overlooked area of research. However, we now turn our attention to reporting the findings of our individualizing comparative analysis of Study C (SC) [84] as to how practitioners navigate such disclosures. This study was based around seven focused group discussions (FGDs) on their understanding of tech abuse; experiences with tech abuse disclosures by APs on APIP programs; and, their perceptions of the risks associated with integrating tech abuse as a topic. For participant anonymity, we associate any APIP professional quotes with P1 – P37.

At a high-level, practitioners reported a *lack of information* about the role of technology on a new referral about an AP, which necessitates a complex process of *verifying ground truth of tech abuse*. APIP practitioners reported a lack of confidence in their technical ability, fearing that discussing tech abuse would lead to *teaching new tactics* to APs by avoiding technology altogether in a session. However, practitioners expressed dismay that they were not equipping APs with *healthy relationships with digital technologies* for sustained behavior change. Such tensions can be understood as causing a ripple effect (Figure 1) across the four high-level chronological phases of APIPs (Section 2).

5.1 Lack of reporting information

APIP providers receive accurate referral information from a variety of sources, including medical staff, law enforcement, social workers, and others. However, many practitioners reported being the

first professional group to learn or at least record instances of tech abuse. As APIPs can act as a secondary referral after interacting with other services, such as law enforcement, many facilitators expressed concern and surprise at being placed in this position. When a lack of further information were provided from such services, facilitators reported being directly reliant on APs for further insight:

> *"often we're left being the detectives ... in the early days it's hard to get them to admit to anything, but we've worked around this by asking at the start of each session if they used technology to harm someone recently ... they share eventually, but we shouldn't really be hearing this vital information from them."* (P5, SC)

To combat this risk, practitioners reported relying on integrated safety support (ISS) workers for further information. ISS workers are professionals who provided separate support, safety planning, and APIP information to survivors who were often able to share a survivor's account of experiencing tech abuse. However, if an ISS worker shared that an AP had been using tech abuse against a survivor which an AP they had not admitted to, or was denying, this could also place an APIP practitioner in a reportedly *"sticky situation"* (P2, SC). As an example, a practitioner (P17, SC) shared a personal anecdote where they had learned about an AP controlling the use of a shared device with a survivor. However, they could not confront the AP directly with this knowledge without jeopardizing a survivor's safety, such as by an AP escalating their control to prevent them from sharing their account [79].

5.2 Inability to verify ground-truth accounts

In addition to feeling under-equipped with knowledge about tech abuse from referral forms, most professionals reported believing that APs were more *"tech savvy"* or *"techy"* (P15, SC) than survivors [15, 31], and occasionally themselves. In response to being asked if they had personal experience of hearing a disclosure by an AP of tech abuse by an AP, a practitioner (P5) reported that an AP had boasted to installing spyware on his former partner's devices (a common fear in IPV service contexts [6, 30, 85, 98]). In their attempt to learn more about spyware online, the practitioner then went on to share encountered either inaccurate or sensationalized media reports:

> *"when I looked online, all I was finding was anti-spyware tool adverts, or even adverts* ***for*** *spyware tools which was very scary ... I just wanted a clear breakdown of if installing spyware without touching her [survivor] device was even possible ..."* (P5, SC)

Practitioners nevertheless continuously underlined the importance of building trust and rapport with APs. This had to be done in a non-judgemental manner to help build environments where they could be respectfully challenged on their behavior. However, such relationships could be easily undermined if an AP sensed that a professional was skeptical or dismissive about their experiences; such as their technical proficiency at being able to install spyware or an equivalent. As practitioners described that manually going through an AP's phone to collect evidence of tech abuse was *"out of the question"* (P7, SC), as many APIPs present themselves as non-punitive and respecting of the AP's privacy outside of the context of an immediate safeguarding risk. Instead, practitioners argued that treating the AP's reports as untrustworthy could lead to disengagement, frustration, and leaving the APIP entirely – an identified risk factor in the re-uptake of abusive behavior [95].

5.3 Providing new tools and tactics

Insecurity around technological competency may also lead facilitators to fear inadvertently providing APs with new ideas or suggestions for ways they could abuse current or former partner(s). Practitioners shared that merely discussing tech abuse could equip an AP with the *idea* of using technology to harm, or such low-level details could be used as step-by-step instructions for an

attack. The concern around providing APs with fresh and detailed descriptions on how to use tech abuse proved to be so powerful that many practitioners admitted to avoiding tech abuse entirely in APIPs. In response to being asked why tech abuse did not feature in their APIP, one practitioner stated: *"we're here to prevent risks to the [survivor], not equip them with tools to be able to better abuse them"* (P17, SC). Nevertheless, not discussing tech abuse at all left many APIP professionals with feelings of embarrassment or shame. As one practitioner shared, to not directly challenging a method of abuse was equivalent to considering it as being acceptable or tolerated:

> *"We need to do better to address the [tech] abuse, the threats ... and I don't dismiss it entirely when it comes up but we go into depth about sexual abuse, physical abuse, parental ... why not tech abuse?"* (P1, SC)

Informing APs of new methods or inspiration to harm survivors has been raised by prior CSCW, HCI, and CS works (e.g., [31, 85]), where low-level details of technical attacks are excluded from published works to reduce the risk of educating adversarial readers. Nevertheless, this is the first time (to our knowledge) that this concern of misidentifying the right *level* of detail in reporting has held trained professionals back from discussing tech abuse directly with APs.

5.4 Discouraging positive tech use

The combination of many of these challenges lead some practitioners to share that they had noticed a reduction or cessation in the healthy uses of digital technologies by an AP. As a result, professionals often discussed the appropriate time to discuss and therefore "de-normalize" tech abuse to ensure that APs engaged in meaningful conversations with other members of the group. After all, as one professional put it, they were hesitant to *"demonize all uses of technology"* (P10, SC), especially when APs were using technologies for positive purposes. These examples included seeing pictures of their children as motivation for behavior change (P10, SC), being responsive to last minute childcare changes via text (P29, SC), and identifying communities of support online (P1, SC). As one facilitator reflected:

> *"... it isn't the tech that's doing the abusing ... tech is just what they can get their hands on, part of [a] wider [set of] strategies of harm and abuse, too much focus on it gives off the impression it is entirely separate."* (P2, SC)

APIP practitioners as such accredited both philosophical and practical challenges in working to communicate the harm of tech abuse in their program materials. Specifically, while many recommendations to give up technology entirely have been criticized by practitioners who work with survivors [27], APIP facilitators have also criticized approaches that recommend similar recommendations for APs.

6 DISCUSSION AND CONCLUDING REMARKS

Our findings simultaneously extend two poignant areas of HCI; by offering in-person, firsthand perspectives from APs on tech abuse [6, 85, 91], and, by providing insight for community-based approaches to mitigating harm [29, 62]. Our research findings shed light on how APs can portray themselves as victims (as seen across other abuse contexts [44, 71, 93]) and judge socially acceptable forms of technology abuse, leading to a better understanding of how discussions about tech abuse can arise in these situations. Yet, simply characterizing technology abuse disclosures (Section 4.1) and how these may change over time (Section 4) is clearly insufficient for APIP practitioners to effectively tackle the numerous challenges that we also surface in our work (Section 5). As designing appropriate responses to mitigate the harms of digital technologies is of rapidly growing interest

to the HCI and CSCW community [10, 26, 29], we now contextualize our findings into recommendations for working with technology abusers in research (Section 6.1), in practice (Section 6.2), and interventions for the APIP ecosystem (Section 6.3).

6.1 Strategies for deriving threat intelligence from APIPs

This research is part of a larger body of work in HCI and CSCW that recognizes the intrinsic value of adversaries' perspectives as sources of information [6, 85]. We confirm Bellini et al. [6] hypothesis that APs did narrate their experiences of tech abuse in substantially different ways to online contexts. While our accounts in this work were rich, we read that when APs were put on the spot in these studies and asked how and if digital technologies played a role in augmenting their abuse, many APs failed to easily articulate exactly how, when and where technology was involved. While it might be easy to approach their confusion or ignorance of the topic as another discursive technique to distance themselves from the use of technology [44], we posit that something else may be at play. We contemplate the difficulty of answering that question, given the pervasive nature of technology in daily life, making it challenging to differentiate what is technology-based and what is not. APs may be managing a significant level of shame and stigma at being seen to use such behaviors, and being provided the right environments to critically explore one's use of technology abuse clearly proved to be inherently valuable for some attendees. Thus, we posit that careful lines of questioning that asks how such harms were achieved, rather than starting with a focus on technology may be a way of bridging this challenge.

Our analyses show that APs' responses to questions about technology abuse are heavily influenced by their social setting. Identifying that APs acknowledge that physical or 'protective' forms of abuse are permissible to admit to in a wider group, while other forms of abuse can incur intense forms of judgement [42, 43]. While this effect could be representative of changing social norms on social surveillance [39, 97], this does nevertheless highlight that researchers should be cautious to derive any prevalence data through firsthand approaches so as not to risk over-representing the prevalence of specific forms of technical attacks. However, what was even more crucial in this work was noticing the facilitator's role in preventing a AP from colluding with others and instead encouraging them to disclose incidents of tech abuse. From a research perspective, such disclosures would have been invaluable insights into the step-by-step nature of some technology attacks (as seen in Tseng et al. [85], or how AP decide to prioritise some attacks over another. Nonetheless, in order to prioritize safeguarding and prevent collusion (Section 3.2), it is vital that APIP facilitators have the ability to interrupt abusers from adversarial learning irrespective of how valuable the insight may be to research. Thus APIPs may not be the most valuable area for eliciting new types of technical attacks due to this interruption effect, but instead highlight invaluable group attitudes on such attacks, and, perhaps more vitally, the strategies for desistance that APs may consider to be most effective.

6.2 Characterizing differences between technology abusers

Our research complements prior work that demonstrate technology attacks may also be characterized by different stages of intensity [83], or progression [6]. Our comparative analysis was not purposed to codify and differentiate different forms of APs, yet our findings show there were stark differences in how APs described using specific forms of technology abuse. While some APs would describe 'blowing up' and impulsively smashing a survivor's device, to those who would carefully and methodically surveil their partner's whereabouts over time (Section 4.1). Although the execution of these types of attacks necessitate different behaviors [51], our work suggests that there could be specific characteristics that differentiate APs from each other.

An area we see as holding great potential is to carefully craft typologies of different profiles of APs who participate in technology abuse. While typographies of abuse may be commonplace across both sociology and criminology [46, 67], this conceptual tool has been underutilized across HCI contexts with respect to user types. Thomas et al. offers a valuable taxonomy of the under-scrutinized qualities of online hate and harassment attacks but we suggest that there could be further scope to explore the unique qualities of the people behind such attacks. Bellini et al. [6] and Lee et al. [51] show initial signs of asking similar questions: *What factors or circumstances directly impact thinking patterns regarding technology misuse?, What motivators help an AP to abstain from participating in technology misuse?*

Constructing such a typology will necessitate several important extensions to this work; namely, via a thorough further in-depth study with APs firsthand, secondary sources of data, standardized measures of technology abuse, and a representative international sample of APs who have used technology abuse. For such a typology to be valid, firsthand in-person APs, once collected should be cross-referenced between other sources of data, which may include case notes, police reports, and even technical logs should evidence gathering procedures for technology-based attacks improve. Next, such interpretations of technology abuse with APs should be collected in a standardized manner, to ensure consistency in a predetermined, standard manner. Finally, our study, while the largest study of AP perspectives on technology abuse to date, is still predominantly focused on Western context which precludes claims of generalizability. Future work may wish to cast a wider net around sampling APs who participate in technology abuse, which may provide further opportunities to identify country-based differences between specific forms of perpetration.

6.3 Bolstering community-based tech abuse prevention efforts

Our findings directly extend existing work that discusses the challenges that tech abuse introduces to practitioners working with survivors [32, 39, 76]. Technologists may be tempted to design entirely new forms of educative digital initiatives to approach this oversight — such as one-off training programmes. Nevertheless, APIPs are already built on decades of practice-based knowledge and are responsive to the violence that occur in their local communities [62]. Importantly, APIPs also necessitate careful coordination with an ISS worker for each survivor connected to an AP on a program; to ensure a survivor is supported, and informed of changes in progress or risk [96]. Our study does not claim to have all the answers and demonstrates the deep complexities to these challenges. We are nevertheless motivated to investigate how APIPs can be used to address tech abuse.

Our chronology of barriers indicated, like most other stakeholder studies of IPV ecosystems [32], that few if any of our field-sites were able to identify and investigate tech abuse in the early stages of intake. Our study highlights that when practitioners are not equipped with this knowledge from the start that this has a ripple effect on *intensifying* other tensions; namely, being unable to investigate or ask an AP directly during evaluation or risk the concern of collusion between other groups members [37, 59, 61, 62]. A self-reported risk assessment for this style of attack (as recommended by [32]) may seem like a sensible first step. However, separating technology from non-technology based attacks presents a philosophical and conceptual challenge [25] which may lead to confused conclusions or outcomes. Our findings after all indicate that self-disclosures from APs prove to be significantly influenced by the audience and the type of abuse. APs admissions of non-technical sexual and financial abuse are substantially lower in APIP settings than psychological, physical, and social forms of abuse [3, 35]. To the uninitiated, this could inadvertently lead to conclusions that such forms of abuse are more prevalent, rather than those which are the most socially acceptable to admit to using. Finally, as APIPs described being less 'tech savvy' than the men, this also could run the risk of when an AP admits to launching a highly-technical attack against a survivor as a

means of scaring a survivor into compliance and it be taken at face value can lead to a substantial amount of time being taken up investigating an attack that is not technically possible.

We anticipate that a form of protocol for data collection that is commonly used by survivors could be viable in such contexts [52]. APs could be encouraged to converse with a trained professional to discuss the presence of tech abuse or attain ground truth of the types of claims offered by an AP. A valuable first starting point for practitioners could be the *understand-investigate-advise* framework of *clinical computer security* [40]. A professional may work to *understand* an AP's account of tech abuse; carefully *investigate* through cross-referencing multiple sources of information; and *advise*an AP on how to desist from such behaviors.

ACKNOWLEDGMENTS

Thank you to all our participants who graciously shared their experiences to benefit research for safer technology development. In addition, we would like to thank our associate chairs and reviewers, whose comments helped improve this manuscript. This work was funded in part by NSF Award #1916096.

LITERATURA

[1] Mariam Asad. 2019. Prefigurative Design as a Method for Research Justice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 200:1–200:18. https://doi.org/10.1145/3359302

[2] Elizabeth A. Bates and Julie C. Taylor. 2019. *Intimate Partner Violence: New Perspectives in Research and Practice*. Routledge. Google-Books-ID: XwaQDwAAQBAJ.

[3] Rosanna Bellini. 2023. Paying the Price: When Intimate Partners Use Technology for Financial Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3544548.3581101

[4] Rosanna Bellini, Simon Forrest, Nicole Westmarland, Dan Jackson, and Jan David Smeddinck. 2020. Choice-Point: Fostering Awareness and Choice with Perpetrators in Domestic Violence Interventions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376386

[5] Rosanna Bellini, Jay Rainey, Andrew Garbett, and Pamela Briggs. 2019. Vocalising Violence: Using Violent Mens' Voices for Service Delivery and Feedback. In *Proceedings of the 9th International Conference on Communities & Technologies - Transforming Communities (C&T '19)*. Association for Computing Machinery, New York, NY, USA, 210–217. https://doi.org/10.1145/3328320.3328405

[6] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (Jan. 2021), 210:1–210:27. https://doi.org/10.1145/3432909

[7] Rosanna Bellini and Nicole Westmarland. 2021. A problem solved is a problem created: the opportunities and challenges associated with an online domestic violence perpetrator programme. *Journal of Gender-Based Violence* 5, 2 (June 2021). https://doi.org/10.1332/239868021X16171870951258 Publisher: Policy Press.

[8] Rosanna Bellini and Nicole Westmarland. 2022. "We adapted because we had to." How domestic violence perpetrator programmes adapted to work under COVID-19 in the UK, the US and Australia. *Journal of Aggression, Conflict and Peace Research* 14, 3 (2022). https://www.emerald.com/insight/publication/issn/1759-6599 Number: 3 Publisher: Emerald.

[9] Rosanna Bellini, Alexander Wilson, and Jan David Smeddinck. 2021. Fragments of the Past: Curating Peer Support with Perpetrators of Domestic Violence. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–14. https://doi.org/10.1145/3411764.3445611

[10] Rosanna Frances Bellini. 2021. *Mechanisms of moral responsibilities: Designing and deploying digital technologies for perpetrators of domestic violence*. Thesis. Newcastle University. http://theses.ncl.ac.uk/jspui/handle/10443/5486 Accepted: 2022-07-04T10:41:24Z.

[11] Rosanna Frances Bellini. 2021. *Mechanisms of moral responsibilities: Designing and deploying digital technologies for perpetrators of domestic violence*. Thesis. Newcastle University.

[12] Rasika Bhalerao, Nora McDonald, Hanna Barakat, Vaughn Hamilton, Damon McCoy, and Elissa Redmiles. 2022. Ethics and Efficacy of Unsolicited Anti-Trafficking SMS Outreach. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 358:1–358:39. https://doi.org/10.1145/3555083

[13] Lindsay Blackwell, Mark Handel, Sarah T. Roberts, Amy Bruckman, and Kimberly Voll. 2018. Understanding "Bad Actors"Online. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3170427.3170610

[14] Chris Bopp and Amy Voida. 2020. Voices of the Social Sector: A Systematic Review of Stakeholder Voice in HCI Research with Nonprofit Organizations. *ACM Transactions on Computer-Human Interaction* 27, 2 (March 2020), 9:1–9:26. https://doi.org/10.1145/3368368

[15] Megan Lindsay Brown, Lauren A. Reed, and Jill Theresa Messing. 2018. Technology-Based Abuse: Intimate Partner Violence and the Use of Information Communication Technologies. In *Mediating Misogyny: Gender, Technology, and Harassment*, Jacqueline Ryan Vickery and Tracy Everbach (Eds.). Springer International Publishing, Cham, 209–227. https://doi.org/10.1007/978-3-319-72917-6_11

[16] Eleanor R. Burgess, Elizabeth Kaziunas, and Maia Jacobs. 2022. Care Frictions: A Critical Reframing of Patient Noncompliance in Health Technology Design. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 281:1–281:31. https://doi.org/10.1145/3555172

[17] Centers for Disease Control and Prevention. 2022. Intimate Partner Violence. https://www.cdc.gov/violenceprevention/intimatepartnerviolence/index.html

[18] Centre for Disease Control and Prevention. 2010. *National Intimate Partner and Sexual Violence Survey.* Technical Report. Centre for Disease Control and Prevention.

[19] Stevie Chancellor, Eric P. S. Baumer, and Munmun De Choudhury. 2019. Who is the "Human"in Human-Centered Machine Learning: The Case of Predicting Mental Health from Social Media. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 147:1–147:32. https://doi.org/10.1145/3359249

[20] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. 441–458. https://doi.org/10.1109/SP.2018.00061 ISSN: 2375-1207.

[21] Chola Chhetri and Vivian Genaro Motti. 2022. User-Centric Privacy Controls for Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 349:1–349:36. https://doi.org/10.1145/3555769

[22] Rachel Clarke, Peter Wright, Madeline Balaam, and John McCarthy. 2013. Digital portraits: photo-sharing after domestic violence. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. Association for Computing Machinery, New York, NY, USA, 2517–2526. https://doi.org/10.1145/2470654.2481348

[23] M. Cowburn. 2005. Confidentiality and public protection: ethical dilemmas in qualitative research with adult male sex offenders. *Journal of sexual aggression* 11, 1 (Jan. 2005), 49–63. https://doi.org/10.1080/13552600512331298284 Number: 1.

[24] Malcolm Cowburn. 2013. Men Researching Violent Men: Epistemologies, Ethics and Emotions in Qualitative Research. In *Men, Masculinities and Methodologies*, Barbara Pini and Bob Pease (Eds.). Palgrave Macmillan UK, London, 183–196. https://doi.org/10.1057/9781137005731_14

[25] Dana Cuomo and Natalie Dolci. 2021. New tools, old abuse: Technology-Enabled Coercive Control (TECC). *Geoforum* 126 (Nov. 2021), 224–232. https://doi.org/10.1016/j.geoforum.2021.08.002

[26] Jessa Dickinson, Jalon Arthur, Maddie Shiparski, Angalia Bianca, Alejandra Gonzalez, and Sheena Erete. 2021. Amplifying Community-led Violence Prevention as a Counter to Structural Oppression. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 180:1–180:28. https://doi.org/10.1145/3449279

[27] Jill P. Dimond, Casey Fiesler, and Amy S. Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5 (Sept. 2011), 413–421. https://doi.org/10.1016/j.intcom.2011.04.006

[28] Russell Dobash, Emerson Dobash, Kate Cavangh, and Ruth Lewis. 2000. Confronting Violent Men. In *Home Truths About Domestic Violence: Feminist Influences on Policy and Practice*. Vol. 1. London ; Concord, MA, 289–309.

[29] Sheena Erete, Jessa Dickinson, Alejandra C. Gonzalez, and Yolanda A. Rankin. 2022. Unpacking the Complexities of Community-led Violence Prevention Work. In *CHI Conference on Human Factors in Computing Systems*. 1–15.

[30] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?"Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 202:1–202:24. https://doi.org/10.1145/3359304

[31] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174241

[32] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on human-computer interaction* 1, CSCW (2017), 1–22. Publisher: ACM New York, NY, USA.

[33] Guo Freeman, Samaneh Zamanifard, Divine Maloney, and Dane Acena. 2022. Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (April 2022), 85:1–85:30. https://doi.org/10.1145/3512932

[34] David Gadd. 2003. Reading Between the Lines: Subjectivity and Men's Violence. *Men and Masculinities* 5, 4 (April 2003), 333–354. https://doi.org/10.1177/1097184X02250838 Publisher: SAGE Publications Inc.

[35] David Gadd and Mary-Louise Corr. 2017. Beyond Typologies: Foregrounding Meaning and Motive in Domestic Violence Perpetration. *Deviant Behavior* 38, 7 (July 2017), 781–791. https://doi.org/10.1080/01639625.2016.1197685 Publisher: Routledge _eprint: https://doi.org/10.1080/01639625.2016.1197685.

[36] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[37] Edward W. Gondolf. 2002. Service Barriers for Battered Women With Male Partners in Batterer Programs. *Journal of Interpersonal Violence* 17, 2 (Feb. 2002), 217–227. https://doi.org/10.1177/0886260502017002007 Publisher: SAGE Publications Inc.

[38] Bridget Harris and Delanie Woodlock. 2023. *Technology and Domestic and Family Violence: Victimisation, Perpetration and Responses*. Taylor & Francis. Google-Books-ID: zAumEAAAQBAJ.

[39] Bridget A Harris and Delanie Woodlock. 2019. Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies. *The British Journal of Criminology* 59, 3 (April 2019), 530–550. https://doi.org/10.1093/bjc/azy052

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

[41] Jeff Hearn, Kjerstin Andersson, and Malcolm Cowburn. 2007. *Background Paper on Guidelines for Researchers on Doing Research with Perpetrators of Sexual Violence*. Technical Report. University of Huddersfield. http://eprints.hud.ac.uk/id/eprint/4997/

[42] Jeff Hearn and Linda McKie. 2010. Gendered and Social Hierarchies in Problem Representation and Policy Processes: "Domestic Violence" in Finland and Scotland. *Violence Against Women* 16, 2 (Feb. 2010), 136–158. https://doi.org/10.1177/1077801209355185

[43] Jeff Hearn and D. H. J. Morgan. 1990. *Men, Masculinities & Social Theory*. Unwin Hyman. Google-Books-ID: wrkOAAAAQAAJ.

[44] Jeff R. Hearn. 1998. *The Violences of Men: How Men Talk about and How Agencies Respond to Men's Violence to Women* (1 edition ed.). Sage Publications, London.

[45] Nicola Henry, Asher Flynn, and Anastasia Powell. 2020. Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women* 26, 15-16 (Dec. 2020), 1828–1854. https://doi.org/10.1177/1077801219875821 Publisher: SAGE Publications Inc.

[46] A. Holtzworth-Munroe and G. L. Stuart. 1994. Typologies of male batterers: three subtypes and the differences among them. *Psychological Bulletin* 116, 3 (Nov. 1994), 476–497. https://doi.org/10.1037/0033-2909.116.3.476

[47] Liz Kelly and Nicole Westmarland. 2016. Naming and Defining 'Domestic Violence': Lessons from Research with Violent Men. *Feminist Review* 112, 1 (Feb. 2016), 113–127. https://doi.org/10.1057/fr.2015.52

[48] Yubo Kou, Xinning Gui, Yunan Chen, and Kathleen Pine. 2017. Conspiracy Talk on Social Media: Collective Sensemaking during a Public Health Crisis. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 61:1–61:21. https://doi.org/10.1145/3134696

[49] Sharon Lamb. 1991. Acts Without Agents: An Analysis of Linguistic Avoidance in Journal Articles on Men Who Batter Women. *American Journal of Orthopsychiatry* 61, 2 (1991), 250–257. https://doi.org/10.1037/h0079243

[50] Sharon Lamb. 1999. *The Trouble with Blame: Victims, Perpetrators, and Responsibility*. Harvard University Press. Google-Books-ID: C_Yg5V6kTFQC.

[51] Song Mi Lee, Cliff Lampe, J.J. Prescott, and Sarita Schoenebeck. 2022. Characteristics of People Who Engage in Online Harassing Behavior. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3491101.3519812

[52] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)*. Association for Computing Machinery, New York, NY, USA, 527–539. https://doi.org/10.1145/3322276.3322366

[53] Roxanne Leitão. 2021. Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction* 36, 3 (May 2021), 203–242. https://doi.org/10.1080/07370024.2019.1685883 Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/07370024.2019.1685883.

[54] Harne Lynne and Radford Jill. 2008. *Tackling Domestic Violence: Theories, Policies And Practice: Theories, Policies and Practice*. McGraw-Hill Education (UK). Google-Books-ID: rpJgLOoPYIUC.

[55] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875

[56] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376167

[57] Wendy Moncur. 2013. The Emotional Wellbeing of Researchers: Considerations for Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 1883–1890. https://doi.org/10.1145/2470654.2466248 event-place: Paris, France.

[58] Eric Monteiro, Neil Pollock, Ole Hanseth, and Robin Williams. 2013. From Artefacts to Infrastructures. *Computer Supported Cooperative Work (CSCW)* 22, 4 (Aug. 2013), 575–607. https://doi.org/10.1007/s10606-012-9167-1

[59] David Morran. 2011. Re-education or recovery? Re-thinking some aspects of domestic violence perpetrator programmes. *Probation Journal* 58, 1 (March 2011), 23–36. https://doi.org/10.1177/0264550510388968

[60] David Morran. 2022. Rejecting and retaining aspects of selfhood: Constructing desistance from abuse as a 'masculine' endeavour. *Criminology & Criminal Justice* (Jan. 2022), 17488958211070365. https://doi.org/10.1177/17488958211070365 Publisher: SAGE Publications.

[61] Ellen Pence. 1983. The Duluth Domestic Abuse Intervention Project. *Hamline Law Review* 6 (1983), 247. https://heinonline.org/HOL/Page?handle=hein.journals/hamlrv6&id=255&div=&collection=

[62] Ellen Pence and Michael Paymar. 1993. *Education Groups for Men Who Batter: The Duluth Model*. Springer Publishing Company, New York.

[63] Richard Phillips, Liz Kelly, and Nicole Westmarland. 2013. Domestic violence perpetrator programmes : an historical overview. http://dro.dur.ac.uk/11512/

[64] Christopher G. Pickvance. 2001. Four varieties of comparative analysis. *Journal of Housing and the Built Environment* 16, 1 (2001), 7–28. https://www.jstor.org/stable/41107161 Publisher: Springer.

[65] Hawra Rabaan, Alyson L. Young, and Lynn Dombrowski. 2021. Daughters of Men: Saudi Women's Sociotechnical Agency Practices in Addressing Domestic Abuse. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (Jan. 2021), 224:1–224:31. https://doi.org/10.1145/3432923

[66] Charles C. Ragin. 1987. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*. University of California Press. https://www.jstor.org/stable/10.1525/j.ctt1pnx57

[67] Carolyn B. Ramsey. 2015. The Stereotyped Offender: Domestic Violence and the Failure of Intervention. *Penn State Law Review* 120 (2015), 337–420. https://heinonline.org/HOL/P?h=hein.journals/dlr120&i=379

[68] Lauren A. Reed, Richard M. Tolman, and L. Monique Ward. 2016. Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students. *Violence Against Women* 22, 13 (Nov. 2016), 1556–1576. https://doi.org/10.1177/1077801216630143 Publisher: SAGE Publications Inc.

[69] Respect. 2021. Respect Standard Accreditation for work with perpetrators of domestic abuse. https://www.respect.uk.net/pages/64-respect-standard

[70] Jennifer A. Rode and Erika Shehan Poole. 2018. Putting the gender back in digital housekeeping. *Proceedings of the 4th Conference on Gender & IT - GenderIT '18* (2018), 79–90. https://doi.org/10.1145/3196839.3196845 Conference Name: the 4th Conference ISBN: 9781450353465 Place: Heilbronn, Germany Publisher: ACM Press.

[71] Patrizia Romito. 2008. *A deafening silence: Hidden Violence Against Women and Children* (1 edition ed.). Policy Press, Bristol.

[72] Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. 2020. The Many Kinds of Creepware Used for Interpersonal Attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*. 626–643. https://doi.org/10.1109/SP40000.2020.00069 ISSN: 2375-1207.

[73] Margarete Sandelowski, Sharron Docherty, and Carolyn Emden. 1997. Qualitative metasynthesis: Issues and techniques. *Research in Nursing & Health* 20, 4 (1997), 365–371. https://doi.org/10.1002/(SICI)1098-240X(199708)20:4<365::AID-NUR9>3.0.CO;2-E _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/%28SICI%291098-240X%28199708%2920%3A4%3C365%3A%3AAID-NUR9%3E3.0.CO%3B2-E.

[74] Julia Slupska. 2019. Safe at Home: Towards a Feminist Critique of Cybersecurity. *St Antony's International Review* 15, 1 (May 2019), 83–100.

[75] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. 2021. Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–6. https://doi.org/10.1145/3411763.3451731

[76] Julia Slupska and Angelika Strohmayer. 2022. Networks of Care: Tech Abuse Advocates' Digital Security Practices. 341–358. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks

[77] Neil J. Smelser. 2013. *Comparative Methods in the Social Sciences*. Quid Pro Books. Google-Books-ID: XfVBzRaAV_oC.

[78] Robert Soden, David Ribes, Seyram Avle, and Will Sutherland. 2021. Time for Historicism in CSCW: An Invitation. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 459:1–459:18. https://doi.org/10.1145/3479603

[79] Evan Stark. 2009. *Coercive Control: The Entrapment of Women in Personal Life*. Oxford University Press. Google-Books-ID: 8h0TDAAAQBAJ.

[80] Angelika Strohmayer, Mary Laing, and Rob Comber. 2017. Technologies and Social Justice Outcomes in Sex Work Charities: Fighting Stigma, Saving Lives. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3352–3364. https://doi.org/10.1145/3025453.3025615

[81] Cris M. Sullivan. 2018. Understanding How Domestic Violence Support Services Promote Survivor Well-being: A Conceptual Model. *Journal of Family Violence* 33, 2 (Feb. 2018), 123–131. https://doi.org/10.1007/s10896-017-9931-6

[82] The United States Department of Justice. 2019. Domestic Violence. https://www.justice.gov/ovw/domestic-violence

[83] 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. 2021. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*. 247–267. https://doi.org/10.1109/SP40001.2021.00028 ISSN: 2375-1207.

[84] Charles Tilly. 1984. *Big Structures, Large Processes, Huge Comparisons*. Russell Sage Foundation. https://www.jstor.org/stable/10.7758/9781610447720

[85] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX Security Symposium (USENIX Security 20)*. 1893–1909.

[86] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3411764.3445589

[87] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–20. https://doi.org/10.1145/3491102.3502038

[88] Sarah Turner, Nandita Pattnaik, Jason R.C. Nurse, and Shujun Li. 2022. "You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 269:1–269:34. https://doi.org/10.1145/3555159

[89] F. Vera-Gray. 2017. 'Talk about a Cunt with too Much Idle Time': Trolling Feminist Research. *Feminist Review* 115, 1 (March 2017), 61–78. https://doi.org/10.1057/s41305-017-0038-y Publisher: SAGE Publications.

[90] Jenny Waycott, Cosmin Munteanu, Hilary Davis, Anja Thieme, Wendy Moncur, Roisin McNaney, John Vines, and Stacy Branham. 2016. Ethical Encounters in Human-Computer Interaction. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, San Jose California USA, 3387–3394. https://doi.org/10.1145/2851581.2856498

[91] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2022. {Anti-Privacy} and {Anti-Security} Advice on {TikTok}: Case Studies of {Technology-Enabled} Surveillance and Control in Intimate Partner and {Parent-Child} Relationships. 447–462. https://www.usenix.org/conference/soups2022/presentation/wei

[92] Nicole Westmarland. 2015. *: Criminological perspectives on men's violences*. Routledge, London. https://doi.org/10.4324/9781315768830

[93] Nicole Westmarland. 2015. *Violence against Women: Criminological perspectives on men's violences* (1 edition ed.). Routledge, London ; New York.

[94] Nicole Westmarland, Mariann Hardey, Hannah Bows, Dawn Branley, Mehzeb Chowdhury, Katie Wheatley, and Richard Wistow. 2013. *Protecting Women's Safety? The use of smartphone 'apps' in relation to domestic and sexual violence*. SASS Research Briefing no. 12. School of Social Sciences, University of Durham. 1–6 pages. https://www.dur.ac.uk/resources/sass/research/briefings/ResearchBriefing12-ProtectingWomensSafety.pdf

[95] Nicole Westmarland and Liz Kelly. 2013. Why Extending Measurements of 'Success' in Domestic Violence Perpetrator Programmes Matters for Social Work. *The British Journal of Social Work* 43, 6 (Sept. 2013), 1092–1110. https://doi.org/10.1093/bjsw/bcs049

[96] Nicole Westmarland and Liz Kelly. 2023. *Standards for domestic abuse perpetrator interventions (accessible)*. Technical Report. London. https://www.gov.uk/government/publications/standards-for-domestic-abuse-perpetrator-interventions/standards-for-domestic-abuse-perpetrator-interventions-accessible

[97] Delanie Woodlock. 2017. The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women* 23, 5 (April 2017), 584–602. https://doi.org/10.1177/1077801216646277 Publisher: SAGE Publications Inc.

[98] Delanie Woodlock, Mandy McKenzie, Deborah Western, and Bridget Harris. 2020. Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control. *Australian Social Work* 73, 3 (July 2020), 368–380. https:

//doi.org/10.1080/0312407X.2019.1607510 Publisher: Routledge _eprint: https://doi.org/10.1080/0312407X.2019.1607510.

[99] Elizabeth Yardley. 2021. Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework. *Violence Against Women* 27, 10 (Aug. 2021), 1479–1498. https://doi.org/10.1177/1077801220947172 Publisher: SAGE Publications Inc.

Received January 2023; revised July 2023; accepted November 2023