Tech Abuse Personas: Exploring Help-Seeking Behaviours and Support Needs of Victim/Survivors of Technology-Facilitated Abuse

Madeleine Janickyj*
Computer Science
University College London
London, United Kingdom
m.janickyj@ucl.ac.uk

Leonie Maria Tanczer*
Computer Science
University College London
London, United Kingdom
l.tanczer@ucl.ac.uk

Abstract

Technology-facilitated abuse (tech abuse) refers to the misuse of digital systems and features to perpetrate other 'traditional' forms of violence in increasingly complex ways. This phenomenon presents critical challenges for human-computer interaction (HCI) researchers, government officials, front-line practitioners, and support organisations. In this study, we analyse 1525 referrals (i.e., someone is directed to or contacts a specialised organisation) made between April 2019 and September 2024 to the UK-based domestic abuse charity *Refuge* focusing on experiences of tech abuse and associated help-seeking behaviours. Using quantitative and inductive analyses, we derive seven distinct personas that capture diverse circumstances, challenges, and support avenues faced by individuals. These personas offer actionable insights into the design of interventions, digital platforms, and support systems that prioritise user safety. Our findings underscore the urgent need for inclusive, survivor-centred approaches in the development of technology, tools and policies to mitigate the harm of tech abuse and improve help-seeking.

CCS Concepts

• **Security and privacy** → *Social aspects of security and privacy.*

Keywords

Technology-Facilitated Abuse, Third-sector Support Services, Help-seeking behaviours, Personas

ACM Reference Format:
Madeleine Janickyj and Leonie Maria Tanczer. 2025. Tech Abuse Personas: Exploring Help-Seeking Behaviours and Support Needs of Victim/Survivors of Technology-Facilitated Abuse. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3706599.3719986

*Both authors contributed equally to this research.

CHI EA '25, Yokohama, Japan

ACM ISBN 979-8-4007-1395-8/25/04
https://doi.org/10.1145/3706599.3719986

1 INTRODUCTION

Technology-facilitated abuse, or tech abuse, defines the misuse of technology to perpetrate more 'traditional' forms of abuse, such as intimate partner violence. These technologies span from 'everyday' connected devices such as mobile phones and laptops to smart home systems and the creation of deepfakes using Artificial Intelligence [9, 48, 50]. As the prevalence of tech abuse rises [40], so too does the demand for specialised support services to assist victim/survivors [90]. These organisations are not only providing essential help such as counselling, legal aid, and refuge, but are also becoming experts in navigating the technological risks faced by victims [84, 107]. Indeed, dedicated teams *within* but also *outside* these organisations are emerging [76, 96] focused on providing tailored tools for securing devices, combating online financial abuse, and empowering affected parties to (re-)take control of their accounts [43, 69, 93, 111].

Building upon the growing recognition of tech abuse [34, 92, 100], there is a parallel body of research focused on understanding the help-seeking behaviours of victim/survivors and how support services can more effectively address their needs [100, 101]. Help-seeking behaviours describe the steps taken by individuals to seek help/support, a concept explored across a wide range of fields, including healthcare, finance, and gender studies [21, 37, 54, 71]. Examining help-seeking behaviours in the context of tech abuse is critical to shed light on the complex obstacles victim/survivors encounter when accessing support [58, 108]. These behaviours illuminate how technology-facilitated harm intersects with support systems, uncovering opportunities to develop interventions that prioritise safety and accessibility [65]. Our work offers complementary insights into designing tools that address these nuanced needs, advancing the conversation on effective technological solutions.

2 Related Work

Tech abuse is increasingly recognised as a critical facet of domestic and intimate partner violence [32, 67]. Researchers, practitioners, and policymakers strive to understand its methods [86, 94], victims/perpetrators [1], and consequences [28, 64]. Scholars like Bellini et al. [5], Redmiles et al. [75] and Slupska et al. [85] have shown how the breadth of technology currently developing has, in turn, created a multitude of avenues for abuse, such as the use of social media, online banking, and Internet of Things (IoT) devices. The diversification of these harms has intensified calls to establish clear definitions [48, 106], robust measurement frameworks [63], and actionable interventions, such as embedding Safety-by-Design principles into technology development [17]. Despite these efforts,

significant gaps remain in addressing the intersection of technology and abuse, particularly concerning the lived experiences of victim/survivors and the systemic factors enabling such misuse.

As technology becomes a central feature of abusive relationships, understanding help-seeking behaviours has gained urgency. Research highlights the varied and intersectional needs of victim/survivors, including men [47], ethnic minorities [27], individuals in the Global South [79], and LGBTQ+ communities [80]. Studies have examined typical support pathways, barriers to accessing help, and the effectiveness of interventions [30, 41]. Recent advancements have focused on reducing the burden on victim/survivors through technology-driven solutions. These include machine learning models to detect abuse [19], chatbots facilitating disclosure and resource access [110], and tools for flagging/obfuscating sensitive images online [51]. However, a pressing demand remains for a nuanced, evidence-based design that centres on victim/survivors' perspectives and considers the broader support ecosystem.

This paper addresses these gaps by analysing the help-seeking behaviours of victim/survivors of tech abuse using data from the United Kingdom (UK)-based support service, *Refuge*. We categorise these behaviours through data-driven personas, offering an evidence-based understanding of the types of tech abuse experienced and their relationship to support-seeking strategies. Persona-driven work using quantitative data from existing records is necessary to challenge the notion of a single victim/survivor experience. It allows us to emphasise how diverse pathways to support are shaped by individual needs and circumstances. By linking these personas with the well-being outcomes of the victim/survivors, we provide actionable guidance for designing interventions that improve safety, accessibility, and efficacy. This work contributes novel empirical evidence to the discourse on tech abuse and establishes a foundation for developing victim-centred, technology-informed solutions.

3 METHOD

3.1 Data

This paper utilises data from the UK domestic abuse charity *Refuge*, which operates the national domestic abuse helpline. In 2018, *Refuge* created a dedicated tech abuse team to deal with the growth of abuse cases involving technology [39]. As part of this initiative, victim/survivors referred to *Refuge* provide information on their experiences of abuse, broader circumstances, and help-seeking behaviours. This process is detailed in Appendix A. The information *Refuge* gathers on help-seeking includes the type of support needed, whether they have sought help previously, and which acts of support made them feel safer. While we had limited access to demographic information, certain data points were available, including: (1) the perpetrator's gender identity, (2) the relationship between the victim/survivor and perpetrator, (3) the victim/survivor's immigration status, (4) the victim/survivor's parental responsibilities, and (5) whether the perpetrator had been in the armed forces. Most questions offered closed-ended responses, with some allowing further elaboration under 'Other'; however, the associated free-text responses were not included in our dataset. The only open-ended questions we had access to focused on help-seeking. Prior to analysis, duplicate records were merged. In total, we reviewed 1525 tech abuse referrals between April 2019 and September 2023, encompassing administrative entry and exit data. Notably, these referrals do not equate to 1,525 individuals but instead 1,478, as some victim/survivors had multiple referrals (i.e., individuals have sought support on more than one occasion). Additionally, some data points were missing due to relevance or victim/survivors' preferences.

3.2 Data Collection

During the referral process, *Refuge*'s front-line workers record victim/survivors' responses—primarily to closed-ended questions—into their SQL database. To maintain anonymity and ensure the data remain non-identifiable, responses are logged under a 'womenID' rather than a client's name. *Refuge*'s assessment included 20 questions explicitly related to technology-facilitated abuse and three concerning help-seeking behaviours. Although these questions cannot be shared due to intellectual property restrictions, they focus on aspects such as the types of technology involved and the specific acts of tech abuse experienced.

3.3 Data Analysis

The responses given by victim/survivors to *Refuge* support workers informed the development of personas. These personas are empirical representations of real victim/survivors which allow us to examine their varied experiences of tech abuse and distinct help-seeking behaviours [62, 78]. Using solely the demographic information available, we identified the most prevalent victim/survivor, which we labelled Persona A - Alex. Alex exemplifies the "average" victim/survivor within this dataset.

We then worked through each of the five demographic questions separately and identified the next most (and in some cases the least) prevalent group. These clusters became Personas B-G, with each persona corresponding to a specific demographic question. An overview of their defining attributes and experiences can be seen in Appendix B, and the number of referrals that informed each persona can be found in Table 1. This inductive approach grounded the personas in actual victim/survivors, offering insight into both the "most common" victim/survivor experiences and those that diverge from the typical [61].

Before we started the analysis, we cleaned responses to the single open-ended question by correcting any clerical errors, removing any responses giving no information (e.g.,'—-'), and categorised support needs, such as securing accounts, devices, or locations, as well as needing specific information or advice. Prevalences were calculated for each persona using Microsoft Excel.

3.4 Ethical Considerations

This study adhered to the highest ethical guidelines to protect victim/survivors. Ethics approval was obtained from the University's Institutional Review Board before beginning the work. Both authors completed safe researcher training and became accredited through the UK Office for National Statistics (ONS) [1] under the Digital Economy Act 2017 (DEA) [68] and completed annual General Data Protection Regulation (GDPR) training. The data exchange process

[1] https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/secureresearchservice/becomeanaccreditedresearcher#full-accredited-researcher-under-the-digital-economy-act-2017-dea-

required extensive legal and procedural arrangements, including a data sharing agreement (DSA) between the charity and researchers, which took over three years to finalise [49, 98]. Once the dataset was shared, it was accessible only through a Trusted Research Environment (TRE) [2] with strict security measures such as encryption to prevent misuse. All data accessed was anonymised, and the researchers never had direct access to *Refuge*'s database. Throughout the study, we collaborated with several front-line organisations, including *Refuge*, who were represented on a project-specific Advisory Board to provide guidance and advice. We maintained continuous communication with *Refuge*'s data and tech abuse teams to ensure the accuracy and integrity of our findings.

4 RESULTS

The analysis of the dataset revealed insights into their experiences of tech abuse, its impacts, and the unique help-seeking behaviours it triggered. While tech abuse is the predominant form of harm, many victim/survivors were subject to other forms of abuse, with psychological abuse being the most prevalent. For most, this presented itself through the monitoring and controlling of technology, whereas those being abused by acquaintances mostly experienced harassment. Notably, a significant proportion of victim/survivors had not previously sought support specifically for tech abuse and were uncertain about their needs before approaching *Refuge*. Among the various forms of abuse, psychological abuse was most frequently disclosed, while sexual abuse was the least likely to be reported. These findings showcase the diverse and individualised nature of abuse experiences, the complex dynamics influencing help-seeking behaviours, and the tailored interventions required to effectively support victim/survivors.

4.1 Seven unique tech abuse experiences and help-seeking behaviours

Within this dataset, we identified seven distinct personas that capture the diverse circumstances and dynamics of tech abuse. The personas are as follows: (A) the most prevalent (or "average") victim/survivor, (B) those not living with their perpetrator and without children, (C) those living with perpetrators who held insecure immigration statuses (i.e., other than UK National, indefinite leave to remain, or settled status), (D) those whose perpetrators were acquaintances, (E) those whose perpetrators were in the armed forces, (F) those experiencing domestic abuse by someone other than a current or ex-partner (i.e., adult family violence), and (G) those with female perpetrators.

4.1.1 Persona A - Alex. Alex represents our most prevalent persona and typifies the "average" victim/survivor. Tech abuse in this persona was perpetrated by the male current or former partner of victim/survivors. They were predominantly UK Nationals, with children, and their perpetrator was not in the armed forces. The most common form of abuse Alex experienced was psychological (98.95%), followed by physical, financial, and sexual abuse (70.06%, 57.76%, and 39.60%, respectively). Mobile phones (i.e., calls and messages) were used to perpetrate most of the abuse (53.95%), followed by social media (11.39%). Other technologies involved location-tracking services, economic systems, and security devices (10.08%, 4.38%, and 3.58%, respectively). Tech abuse acts typically involved monitoring their mobile phone, controlling smart home devices, or depriving them of technology (48.67%). Other notable actions involved harassment (public or private, and towards the victim/survivor's friends, family, or co-workers; 31.55%), financial abuse (withholding money or coerced debt; 10.42%), and image-based abuse (sending images to or of the victim/survivor, including threatening to do so; 5.02%).

Our analysis of help-seeking behaviours also revealed that victim/survivors often disclosed their abuse to only one entity, with the type of abuse shaping their choice of confidant. For example, victim/survivors of financial abuse told family members (27.67%), while those facing physical, sexual, and psychological abuse told police officers (38.00%, 38.75%, and 29.45% respectively). However, regarding their help-seeking of tech abuse, only 5.20% of victim/survivors sought support prior to coming to *Refuge*, underscoring the limited awareness and pathways for addressing this specific form of harm. Reflecting this uncertainty, an overwhelming majority (92.16%) reported not knowing what kind of support they needed. Among those who could articulate their needs, a small fraction sought advice (1.53%) or indicated a general need for support without specifying the type (1.63%). When asked what forms of assistance made them feel safe, victim/survivors emphasised practical interventions. The most impactful support included "securing my accounts" (23.36%), "provided guidance/resources to secure accounts/devices" (22.21%), and "helped secure my location" (11.45%).

4.1.2 Persona B-Bailey. Although Bailey did not live with their perpetrator and did not have any children with them, they experienced similar levels of physical and psychological abuse as Alex (73.93% and 98.57% respectively). They faced less financial abuse (48.56%) but more sexual abuse (48.57%), most often from a male (92.92%) ex-partner (83.49%). While experiencing less monitoring or controlling of technology (41.53%%), they endured higher levels of harassment (36.57%) and image-based abuse (8.80%), often via social media (14.63%). They also expressed greater concern about online privacy (6.77%). Reflecting the nature of their abuse, Bailey's help-seeking often focused on social media—seeking ways to block perpetrators, remove harmful content, and report abuse to the police. Some had sought help for tech abuse before (5.66%) and for most forms of abuse (excluding financial abuse, disclosed to family), they approached the police. Like Alex, key concerns included the abuse worsening (42.99%), or the perpetrator committing lethal violence (14.33%). Securing accounts, devices, and location (29.31%, 23.71%, and 12.93%) were the most beneficial acts of help Bailey received.

4.1.3 Persona C-Charlie. Charlie was more physically dependent on their perpetrator than other personas. Their perpetrator was typically a male (96.77%) partner (64.52%) or ex-partner (35.48%), and they experienced psychological abuse most frequently (100%), followed by high levels of physical (96.67%), financial (90.32%), and sexual (63.33%) abuse. Charlie faced typical levels of abuse via location-tracking apps (8.95%) but more economic abuse (8.62%), with monitoring/controlling behaviours being most prevalent (67.12%). They also experienced higher rates of image-based abuse than others

[2] https://aro.tech/solutions/data-centre-services/professional-services/tre-design-and-implementation/

Table 1: Tech-abuse experiences of the personas A-G, including the *n*-values for each category.

Tech Abuse Behaviour	Full Data	A	B	C	D	E	F	G
n	1525	1058	212	31	8	38	54	51
Harassment	30.97%	31.55%	36.57%	12.33%	57.89%	33.78%	32.17%	38.21%
Monitoring/Controlling	48.69%	48.67%	41.53%	67.12%	31.58%	50.00%	47.83%	43.09%
Economic	10.08%	10.42%	7.90%	9.59%	0.00%	13.51%	11.30%	8.94%
Image-based	5.91%	5.02%	8.80%	9.59%	0.00%	1.35%	3.48%	4.88%
Impersonation	1.83%	1.69%	3.16%	0.00%	5.26%	0.00%	3.48%	3.25%
Other	2.51%	2.65%	2.03%	1.37%	5.26%	1.35%	1.74%	1.63%

within this data (9.59%), often involving threats to share images rather than actual dissemination. Charlie's dependence on their perpetrator was reflected in worries about homelessness (13.11%) and concerns over their children being taken (11.48%) or harmed by the perpetrator (9.84%). Police were most often told about physical and sexual abuse, while family members were confided in about psychological and financial abuse. Few knew what support they needed (3.23%), and Charlie had not sought help for tech abuse before. However, they benefitted from interventions similar to Alex.

4.1.4 Persona D-Dakota. Dakota's experience differed from other victim/survivors as their perpetrator was an acquaintance, which influenced the types of abuse they faced. Their perpetrator, who was predominantly male (75.00%), committed psychological abuse but less frequently engaged in physical or sexual abuse (37.50% and 37.50% respectively). Dakota did not experience financial abuse. Certain platforms, such as social media (27.27%) and dating or gaming sites or apps (13.64%), were more commonly used in their case. Harassment was the most prevalent form of abuse, affecting 57.89% of Dakota's experiences. Regarding help-seeking, Dakota, on average, told more entities of their psychological abuse (1.7) compared to their physical (1) or sexual (1.3) abuse. Again, in all cases, a police officer was most often told. Dakota was one of the examples that did not disclose what support they would need the most but did try to seek support for their tech abuse in the past (12.50%). This could relate to one of Dakota's worries being stalking (23.08%). The most common support Dakota benefited from was "securing my accounts" (25.00%), which correlates with their concerns about stalking and experiences of harassment.

4.1.5 Persona E-Ezra. Ezra's perpetrator, a male in the armed forces (100%), was typically a partner or ex-partner (23.68% and 71.05%, respectively). Ezra was subject to less physical (60.53%) and sexual abuse (31.58%) than the Alex but faced similar levels of financial abuse (57.89%). They were constantly subjected to psychological abuse. In terms of tech abuse, Ezra faced higher levels of location tracking (12.99%) but lower levels of social media abuse (9.09%) compared to the dataset. Monitoring/controlling behaviours were common (50.00%), but they faced slightly more economic abuse (13.51%). Ezra rarely sought help (89.47%), though they mentioned needing general online support (2.63%). They had seldom sought support for tech abuse (5.26%), and Ezra disclosed their abuse to few people, averaging 0.25, 0.5, 1.18, and 1.54 individuals about their sexual, financial, physical and psychological abuse respectively. Help from official organisations, friends, and family was common. Helping Ezra secure their location made them feel safer compared with the general dataset (20.45%), as did helping them secure home devices (4.55%) and supporting their debt management (4.55%).

4.1.6 Persona F-Frankie. Frankie, representing those victim/survivors experiencing "adult family violence," had a male perpetrator (64.81%), typically a parent (44.44%). They faced higher levels of physical (83.33%) and similar levels of psychological (96.15%) and financial abuse (53.85%) compared to the most common victim/survivor, Alex. However, sexual abuse was less common (22.22%). The tech abuse Frankie faced was similar to Ezra, with monitoring/controlling behaviours (47.83%), harassment (32.17%), and economic abuse (11.30%) being most common. Frankie did not try to seek help for their tech abuse but recognised a need for securing accounts/devices (5.36%), financial tech abuse (1.79%), and other general advice (5.36%). In some cases, they knew they needed support but were unsure of what (3.57%) or that they needed 'other' forms of support (9.59%). Regarding their other abuse, they most often told a police officer, but with financial abuse, they told friends. As expected, Frankie did not disclose any of their abuse to a family member.

4.1.7 Persona G-Georgie. Georgie's perpetrator was always female. They were often an ex-partner (45.10%), but the next most common perpetrator was their mother (15.69%). They experienced psychological abuse in all cases, and physical (68.00%) and financial (52.00%) abuse most of the time. Similarly to Frankie, they experienced less sexual abuse (27.45%). Compared to other victim/survivors, Georgie was subjected to more abuse using tracking apps and services (13.91%) and via social media than Alex(19.13%). Relating to this, the behaviours they experienced included controlling technology (38.21%) and harassment (38.21%). Georgie rarely sought help for their tech abuse but most often felt they needed advice or information (11.11%). They disclosed their abuse to more people, particularly police officers or professionals, than other victim/survivors. The most helpful support they received was guidance on securing devices and accounts (25.00%).

5 DISCUSSION

Our analysis underscores the nuanced circumstances of victim/survivors of tech abuse, particularly how their experience with technology shapes their help-seeking behaviours. The findings highlight that many victim/survivors encounter similar abuse tactics, such as monitoring/controlling behaviours and harassment, with some experiencing abuse through specific technologies such as location-tracking apps. Additionally, we found that many victim/survivors

had not sought help before, with the co-occurring abuse types influencing this. The different personas within our study reported varying degrees of understanding and awareness of the support they needed to combat tech abuse, further underlining the complex interplay between technology, help-seeking, and victim/survivor needs.

One of the central findings in this analysis is that many victim/survivors did not seek help for tech abuse before reaching *Refuge*. One possible explanation is the difficulty in recognising tech abuse as a form of violence, compounded by the normalisation of certain behaviours within digital spaces, making them harder to identify as abusive. Studies [35, 59] show that the increasing normalisation of tech-related misuses, such as tracking and harassment via smartphones and apps, complicates both recognition and help-seeking. Furthermore, barriers to help-seeking often include a lack of technical knowledge, difficulty gathering evidence, and a general unawareness of available resources [41]. Wei et al. [103] have shown that sociodemographic factors affect security behaviours. Together, these issues illustrate the complex nature of seeking help for tech abuse, particularly within the context of evolving digital technologies. From an HCI perspective, it is evident that the design of support systems for tech abuse needs to be more nuanced. Digital platforms often lack mechanisms for recognising and addressing abuse that occurs through emerging technologies, like stalkerware [13, 16]. Effective support systems must be designed with an understanding of these barriers and offer tailored solutions for victims who may not even realise they need help [25].

Although tech abuse is a relatively new form of abuse, it frequently co-occurs alongside other types of violence, especially psychological abuse. Compared with the other forms, psychological abuse often does not have the same requirements of being 'physically present' [109]. Because of this, it is often seen as less severe than physical abuse [105] even though it creates a sense of omnipresence for the perpetrators that the victim/survivors cannot escape from [57]. Conversely, we see the least common co-occurrence of abuse here is tech abuse with financial and sexual. However, as seen by O'Malley and Holt [66] there has been an increase in sextortion, an act that involves threatening to share intimate images which can in some cases have financial demands attached to it. So while we do not see instances of these abuse types co-occurring here it is happening and in many cases, victim/survivors don't seek help due to feelings of shame or the belief that no one can help which often leads to symptoms associated with depression and anxiety [74]. The design of technology plays a significant role in this dynamic. For instance, social media platforms can inadvertently facilitate the perpetration of tech abuse [75, 81]. With this, it is clear that technologies must be redesigned to better protect users by both preventing this abuse and offering clear pathways for reporting and support [6, 8, 32, 55, 95].

In our results, we examined who victim/survivors disclosed their abuse to and the number of individuals they confided in. Given psychological abuse was most prevalent, it is fitting that victim/survivors of this abuse told the most people about it. This can often present through harassment, which many adults beyond our dataset experience [99]. As harassment has increased, various response mechanisms have emerged, both within digital platforms and through third-party tools designed to support users [45, 88, 102]. In contrast, sexual tech abuse, was less prevalent and disclosed to fewer individuals. Public perceptions of sexual abuse, particularly image-based abuse, often involve victim-blaming, harm minimisation, and stigma, which are well-documented barriers to help-seeking [29, 52, 73]. These societal attitudes likely contribute to the lower rates of disclosure of sexual abuse compared to psychological abuse, highlighting the complex dynamics that shape victim/survivors' decisions to seek help within digital spaces [73]. Beyond these attitudes we can also see the impact of having built-in reporting mechanisms; the more routes to disclosure that exist within the misused technology the more victim/survivors are able to safely report their abuse and get support [3].

Our findings also highlight that victim/survivors with perpetrators in the armed forces or female perpetrators of tech abuse face unique challenges (e.g., location-tracking apps). While stalkerware and other forms of digital surveillance are becoming increasingly prevalent [18, 46], detecting these tools remains a significant challenge, even with improving detection methods [26, 42]. Victim/survivors may not seek help due to feelings of embarrassment, fear of escalation, or the perception that their experiences aren't "serious" enough [2, 89]. It is also important to consider the perception of abuse by female perpetrators. These acts of violence are thought of as less impactful, less serious, and less intrusive, perceptions which can all impact the help-seeking of victim/survivors of these female perpetrators [11, 104]. This highlights the need for digital platforms to reconsider how they address forms of abuse that may be minimised or overlooked in public discourse. Designing more intuitive and accessible systems for identifying, preventing, and responding to tech abuse must also account for these complex perceptions of severity and gendered dynamics of violence.

Our analysis uncovered the unique challenges faced by victim/survivors of adult family violence, such as those experienced by Frankie, whose abuse trajectory mirrored the broader dataset. Within this group, no one had sought support for tech abuse before. Adult family violence is unique in the sense that it is underresearched compared to abuse in other periods of the life course [82]. These other forms of family violence, such as child and elder abuse, have been shown to have their own unique forms of help-seeking. Pereira et al. [70] showcased how children favour informal reporting while Dominguez, Storey, and Glorney [23] found that barriers to elders seeking support included fear of the consequences, their knowledge of support services, and their perception of the abuse. With this, we see that further research is needed both to raise awareness for victim/survivors of adult family violence but also to anticipate the required support. But, these support systems must be equipped to recognise and assist those facing family-related tech abuse, especially when the abuse is entrenched within complex interpersonal dynamics and the victim/survivors are likely to experience a lack of understanding or inappropriate responses if they do report the abuse [77].

Another critical factor identified in our study is the vulnerability of victim/survivors like Charlie, whose immigration status exacerbates their exposure to financial and tech abuse. For individuals in similar situations, concerns about homelessness, the welfare of their children, and the overwhelming burden of financial dependency on their abuser significantly complicate their ability to seek help. Research has shown that financial abuse, often intertwined

with tech abuse [5], is a significant barrier to escaping abusive relationships, as victim/survivors are financially dependent on their abusers [20, 36]. This dependency makes leaving the relationship exceedingly difficult. Additionally, prior research underscores the detrimental effects of financial insecurity on both security and privacy. In particular, a recent study highlights how financial instability exacerbates these challenges, particularly for those in transitional housing or at risk of homelessness [83]. These findings resonate with our own, illustrating how financial and tech abuse are inextricably linked, particularly for victim/survivors facing compounded vulnerabilities [7, 24, 44].

5.1 Implications for Design and Support Systems

The findings from our study highlight several implications for the design of tech-based support systems for victim/survivors of abuse. First, a significant barrier to help-seeking is how victim/survivors perceive their situations. While efforts to raise awareness of these emerging harms are underway, more must be done to shift the onus from victim/survivors to platforms and digital systems, which should proactively recognise abuse and offer clear response and reporting mechanisms [15, 55]. Second, while victim/survivors of traditional abuse often seek help from police or other agencies, tech abuse lacks the necessary training, recognition, and legislation to provide effective support through these channels [31]. Support systems must anticipate the threats associated with emerging technologies and become equipped to be responsive and future-proof. Methods such as design fiction [10, 38], future and foresight techniques [4, 60, 91], and anticipatory ethnography [53] can help guide this process. Third, many victim/survivors are unsure about the support they need. While some platforms provide "quick exit" buttons [97] and similar features, more must be done in recognition of those who do not have the media literacy or the technology (that is not monitored) to educate themselves about the types of support available [72]. Lastly, technologies must be developed with these victim/survivors in mind. They should consider threat models [85], the UI bound adversary [33], and the possible abuse vectors [86] in their design processes. These considerations will mitigate the risk of these technologies being misused and limit their possible impact on victim/survivors. Overall, foundational research like ours is essential in shaping the design of online spaces and digital tools, ensuring they are rooted in the lived experiences of victim/survivors.

5.2 LIMITATIONS

While our analysis is rigorous, several limitations must be noted. First, our personas, though diverse, may not fully capture the range of victim/survivor experiences [22]. Second, the anonymised dataset lacks demographic details (e.g., age, ethnicity), limiting our ability to explore nuanced differences across groups. Finally, as *Refuge* primarily supports women (including transwomen) and children, the dataset does not include experiences of (trans)men or non-binary individuals.

6 CONCLUSION

This paper has provided a detailed exploration of the diverse experiences of tech abuse and the complex help-seeking behaviours exhibited by victim/survivors. Our findings reveal that tech abuse extends beyond traditional forms of harassment and monitoring through social media and mobile devices, incorporating a range of digital tools and technologies. We have shown how victim/survivors' ability to recognise and seek help for tech abuse is heavily influenced by the nature of the abuse they experience, as well as their dependency on the perpetrator. Both of which silence victim/survivors and complicate pathways to support. Beyond this, our analysis also indicated that the lack of awareness around available support is a critical barrier.

This work contributes to the growing body of research on the intersection of technology and abuse, highlighting the need for targeted interventions and support systems, including introducing more overt methods of intervention [14, 56], more training for support professionals such as police officers to recognise this abuse [87, 90], and more avenues for victim/survivors to educate themselves on the available support [12]. Ultimately, our goal is to foster a more informed, compassionate, and responsive approach to the challenges faced by tech abuse victim/survivors, ensuring that they have the necessary resources and support to reclaim their safety and autonomy.

Acknowledgments

We are deeply grateful to *Refuge* for granting us access to their data, which was essential for completing this research. We extend our heartfelt thanks to the teams we collaborated with throughout this process. A special shout-out goes to Emma Pickering (Head of Technology-Facilitated Abuse and Economic Empowerment), Jessica Eagleton (Head of Policy, Public Affairs and Research) and Kelly Gingell (Head of Data) for their dedication, which has been instrumental in our efforts to represent and respect the victim/survivors they support. We greatly appreciate their invaluable insights and patience in answering our many questions. For those looking to help combat tech abuse, we encourage you to support these vital efforts in any way you can. We are also thankful to the *Gender and Tech Research Lab* at UCL Computer Science for their feedback and celebration of this work.

References

[1] Rojan Afrouz. 2023. The nature, patterns and consequences of technology-facilitated domestic abuse: A scoping review. *Trauma, Violence, & Abuse* 24, 2 (2023), 913–927. doi:10.1177/15248380211046752

[2] Victoria Ameral, Kathleen M Palm Reed, and Denise A Hines. 2020. An analysis of help-seeking patterns among college student victims of sexual assault, dating violence, and stalking. *Journal of Interpersonal Violence* 35, 23-24 (2020), 5311–5335. doi:10.1177/0886260517721169

[3] Emma Bailey. 2020. *Barriers to Reporting Sexual Harassment: What Encourages Disclosure?* Master's thesis. University of Windsor (Canada).

[4] Wendell Bell. 2004. *Foundations of Futures Studies. Volume 1: History, Purposes, and Knowledge.* Transaction Publishers.

[5] 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*. Association for Computing Machinery, New York, NY, USA, 1–17. doi:10.1145/3544548.3581101

[6] Rosanna Bellini, Simon Forrest, Nicole Westmarland, and Jan David Smeddinck. 2020. Mechanisms of Moral Responsibility: Rethinking Technologies for Domestic Violence Prevention Work. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for

Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376693

[7] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. SoK: Safer Digital-Safety Research Involving At-Risk Users. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 635–654. doi:10.1109/SP54263.2024.00071

[8] Arkaprabha Bhattacharya, Kevin Lee, Vineeth Ravi, Jessica Staddon, and Rosanna Bellini. 2024. Shortchanged: Uncovering and Analyzing Intimate Partner Financial Abuse in Consumer Complaints. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 354, 20 pages. doi:10.1145/3613904.3642033

[9] Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. 2022. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 2691–2708. https://www.usenix.org/conference/usenixsecurity22/presentation/blue

[10] Mark Blythe. 2014. Research through design fiction: narrative in real and imaginary abstracts. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 703–712. doi:10.1145/2556288.2557098

[11] Nathan Brooks, Wayne Petherick, Arathi Kannan, Peta Stapleton, and Serena Davidson. 2021. Understanding female-perpetrated stalking. *Journal of threat assessment and management* 8, 3 (2021), 65–76. doi:10.1037/tam0000162

[12] Andi Brown, Diarmaid Harkin, and Leonie Maria Tanczer. 2024. Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence against women* 31, 5 (2024), 10778012231222486. doi:10.1177/10778012231222486

[13] Kevin Butler. 2023. Following the Money: Characterizing the Monetization Ecosystem of Stalkerware Through Application Analysis. USENIX Association, Anaheim, CA.

[14] Esther Calvete, Liria Fernández-González, and Izaskun Orue. 2023. A growth mindset and self-affirmation intervention to reduce violent and risky online behaviors: the moderating role of previous victimization. *Journal of interpersonal violence* 38, 7-8 (2023), 5875–5901. doi:10.1177/08862605221127221

[15] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky spy devices and defective detectors: the ecosystem of intimate partner surveillance with covert devices. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 123–140.

[16] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, CA, USA, 441–458. doi:10.1109/SP.2018.00061

[17] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 544, 20 pages. doi:10.1145/3491102.3517475

[18] Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa M. Redmiles, Eakta Jain, Patrick Traynor, and Kevin R. B. Butler. 2024. "I Had Sort of a Sense that I Was Always Being Watched...Since I Was": Examining Interpersonal Discomfort From Continuous Location-Sharing Applications. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 4197–4211. doi:10.1145/3658644.3690342

[19] Hyojin Chin, Lebogang Wame Molefi, and Mun Yong Yi. 2020. Empathy Is All You Need: How a Conversational Agent Should Respond to Verbal Abuse. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376461

[20] Kameri Christy, Tanice Welter, Kelly Dundon, Valandra, and Ambra Bruce. 2022. Economic abuse: A subtle but common form of power and control. *Journal of Interpersonal Violence* 37, 1-2 (2022), NP473–NP499. doi:10.1177/0886260520916264

[21] Nicola Cornally and Geraldine McCarthy. 2011. Help-seeking behaviour: A concept analysis. *International journal of nursing practice* 17, 3 (2011), 280–288. doi:10.1111/j.1440-172X.2011.01936.x

[22] Sasha Costanza-Chock. 2020. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, Cambridge, Massachusetts. doi:10.7551/mitpress/12255.001.0001

[23] Silvia Fraga Dominguez, Jennifer E. Storey, and Emily Glorney. 2021. Help-Seeking Behavior in Victims of Elder Abuse: A Systematic Review. *Trauma, Violence, & Abuse* 22, 3 (2021), 466–480. doi:10.1177/1524838019860616 arXiv:https://doi.org/10.1177/1524838019860616 PMID: 31291837.

[24] Rebecca Gail Dudley. 2017. Domestic abuse and women with 'no recourse to public funds': The state's role in shaping and reinforcing coercive control. *Families, relationships and societies* 6, 2 (2017), 201–217. doi:10.1332/204674317X14937364476840

[25] Maggie A Evans and Gene S Feder. 2016. Help-seeking amongst women survivors of domestic violence: A qualitative study of pathways towards formal and informal support. *Health Expectations* 19, 1 (2016), 62–73. doi:10.1111/hex.12330

[26] Ruba Taha EyalSalman. 2023. Android Stalkerware Detection Techniques: A Survey Study. In *2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*. IEEE, 270–275. doi:10.1109/JEEIT58638.2023.10185812

[27] Omolade Femi-Ajao, Sarah Kendal, and Karina Lovell. 2020. A qualitative systematic review of published work on disclosure and help-seeking for domestic violence and abuse among women from ethnic minority populations in the UK. *Ethnicity & Health* 25, 5 (2020), 732–746. doi:10.1080/13557858.2018.1447652 arXiv:https://doi.org/10.1080/13557858.2018.1447652 PMID: 29514473.

[28] Renee Fiolet, Cynthia Brown, Molly Wellington, Karen Bentley, and Kelsey Hegarty. 2021. Exploring the impact of technology-facilitated abuse and its relationship with domestic violence: A qualitative study on experts' perceptions. *Global qualitative nursing research* 8 (2021), 2333936211028176. doi:10.1177/23333936211028176

[29] Asher Flynn, Elena Cama, Anastasia Powell, and Adrian J Scott. 2023. Victim-blaming and image-based sexual abuse. *Journal of Criminology* 56, 1 (2023), 7–25. doi:10.1177/26338076221135327

[30] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2021. *Technology-facilitated abuse: A survey of support services stakeholders*. Technical Report. Australia's National Research Organisation for Women's Safety (ANROWS).

[31] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2023. Policing technology-facilitated abuse. *Policing and Society* 33, 5 (2023), 575–592. doi:10.1080/10439463.2022.2159400

[32] 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. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 202 (Nov. 2019), 24 pages. doi:10.1145/3359304

[33] 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*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3173574.3174241

[34] Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. 2022. Analyzing the monetization ecosystem of stalkerware. *Proceedings on Privacy Enhancing Technologies* 22 (2022), 105–119. Issue 4. doi:10.56553/popets-2022-0101

[35] Rosalie Gillett. 2018. Intimate intrusions online: Studying the normalisation of abuse in dating apps. *Women's Studies International Forum* 69 (2018), 212–219. doi:10.1016/j.wsif.2018.04.005.

[36] Jennifer Glinski. 2024. *"You Can't Plan to Leave Under the System": Experiences of economic abuse and seeking support for separation*. Ph. D. Dissertation. University of Glasgow.

[37] John E Grable and So-hyun Joo. 1999. Financial help-seeking behavior: Theory and implications. *Journal of Financial Counseling and Planning* 10, 1 (1999), 14.

[38] Simon Grand and Martin Wiedmer. 2010. Design fiction: a method toolbox for design research in a complex world. In *Design and Complexity - DRS International Conference 2010*.

[39] Womens Grid. 2017. Refuge launches new programme to empower women to tackle technological abuse. https://www.womensgrid.org.uk/?p=4271. Accessed: 23-01-2025.

[40] Naman Gupta, Sanchari Das, Kate Walsh, and Rahul Chatterjee. 2024. A Critical Analysis of the Prevalence of Technology-Facilitated Abuse in US College Students. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 15, 12 pages. doi:10.1145/3613905.3652036

[41] Naman Gupta, Kate Walsh, Sanchari Das, and Rahul Chatterjee. 2024. " I really just leaned on my community for support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of {Technology-Facilitated} Abuse to Seek Social Support. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4981–4998.

[42] Yufei Han, Kevin Alejandro Roundy, and Acar Tamersoy. 2021. Towards Stalkerware Detection with Precise Warnings. In *Proceedings of the 37th Annual Computer Security Applications Conference* (Virtual Event, USA) *(ACSAC '21)*. Association for Computing Machinery, New York, NY, USA, 957–969. doi:10.1145/3485832.3485901

[43] 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)*. USENIX Association, Santa Clara, CA, 105–122.

[44] Zunaira Jamil. 2017. *Monitoring tweets for depression to detect at-risk users.* Ph. D. Dissertation. Université d'Ottawa/University of Ottawa.

[45] Shagun Jhaver, Sucheta Ghoshal, Amy Bruckman, and Eric Gilbert. 2018. Online harassment and content moderation: The case of blocklists. *ACM Transactions on Computer-Human Interaction (TOCHI)* 25, 2 (2018), 1–33. doi:10.1145/3185593

[46] Kaspersky. 2024. *The State of Stalkerware in 2023.* Technical Report. Kaspersky.

[47] Eurosia Yu Yuan Kim, LaRon E Nelson, Travis Lanz-Brian Pereira, and Shefaly Shorey. 2024. Barriers to and facilitators of help-seeking among men who are victims of domestic violence: A mixed-studies systematic review. *Trauma, Violence, & Abuse* 25, 3 (2024), 2189–2203. doi:10.1177/15248380231209435

[48] Nikolaos Koukopoulos, Madeleine Janickyj, and Leonie Maria Tanczer. 2025. Defining and Conceptualizing Technology-Facilitated Abuse ("Tech Abuse"): Findings of a Global Delphi Study. *Journal of Interpersonal Violence* (2025), 08862605241310465. doi:10.1177/08862605241310465 PMID: 39825713.

[49] Shiri Krebs and Lyria Bennett Moses. 2024. Data sharing agreements: Contracting personal information in the digital age. *Melbourne University Law Review* 48, 1 (2024), 95–151.

[50] Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Kevin Butler, and Patrick Traynor. 2024. SoK: the good, the bad, and the unbalanced: measuring structural limitations of deepfake media datasets. In *Proceedings of the 33rd USENIX Conference on Security Symposium* (Philadelphia, PA, USA) *(SEC '24)*. USENIX Association, USA, Article 58, 18 pages.

[51] Yifang Li and Kelly Caine. 2022. Obfuscation remedies harms arising from content flagging of photos. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–25. doi:10.1145/3491102.3517520

[52] Kai Lin, Vincent Shing Cheng, Jessica CM Li, Cindy Xinshan Jia, Xin Jiang, and Budeba Petro Mlyakado. 2025. Online Sexual Exploitation Among Adolescents in Tanzania: Exploring the Stigmas of Victimization and Help-Seeking. *Child & Family Social Work* (2025). doi:10.1111/cfs.13266

[53] Joseph Lindley and Paul Coulton. 2016. Pushing the Limits of Design Fiction: The Case For Fictional Research Papers. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4032–4043. doi:10.1145/2858036.2858446

[54] Julia Luise Magaard, Tharanya Seeralan, Holger Schulz, and Anna Levke Brütt. 2017. Factors associated with help-seeking behaviour among individuals with major depression: A systematic review. *PloS one* 12, 5 (2017), e0176730. doi:10.1371/journal.pone.0176730

[55] Dana McKay and Charlynn Miller. 2021. Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 332, 14 pages. doi:10.1145/3411764.3445114

[56] Gemma McKibbin, Matt Tyler, Esther Gallois, Anneliese Spiteri-Staines, Cathy Humphreys, and Julie Green. 2024. "Frantic online searches for help": design considerations for an online early intervention service addressing harmful sexual behaviour. *Journal of Sexual Aggression* 30, 2 (2024), 246–258. doi:10.1080/13552600.2022.2102682

[57] Freya McLachlan and Bridget Harris. 2022. Intimate risks: examining online and offline abuse, homicide flags, and femicide. *Victims & Offenders* 17, 5 (2022), 623–646. doi:10.1080/15564886.2022.2036658

[58] Georgina Mclocklin, Blerina Kellezi, Clifford Stevenson, and Jennifer Mackay. 2024. Disclosure decisions and help-seeking experiences amongst victim-survivors of non-consensual intimate image distribution. *Victims & Offenders* (2024), 1–27. doi:10.1080/15564886.2024.2329107

[59] Frankie Meade. 2023. Is intimate partner abuse normalised in the digital world? *BPS Branch Awards* (2023), 22. doi:10.53841/bpsba.2023.1.1.22

[60] Ian Miles, Dirk Meissner, Nicholas S Vonortas, and Elias Carayannis. 2017. Technology foresight in transition. 211–218 pages.

[61] Timothy Neate, Aikaterini Bourazeri, Abi Roper, Simone Stumpf, and Stephanie Wilson. 2019. Co-created personas: Engaging and empowering users with diverse needs within the design process. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3290605.3300880

[62] Lene Nielsen. 2013. *Personas-user focused design.* Vol. 15. Springer.

[63] University of Melbourne and United Nations Population Fund. 2023. *Measuring technology-facilitated genderbased violence. A discussion paper.* Technical Report. University of Melbourne and United Nations Population Fund.

[64] Ofcom. 2023. *Qualitative research into the impact of online hate.* Technical Report. Ofcom.

[65] Mairin O'Mahony and Josephine Hegarty. 2009. Help Seeking for Cancer Symptoms: A Review of the Literature. *Oncology nursing forum* 36, 4 (2009), E178–84. doi:10.1188/09.ONF.E178-E184 Copyright - Copyright Oncology Nursing Society Jul 2009; Last updated - 2023-11-30.

[66] Roberta Liggett O'Malley and Karen M Holt. 2022. Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of interpersonal violence* 37, 1-2 (2022), 258–283. doi:10.1177/0886260520909186

[67] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. 2019. Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse. In *Proceedings of the new security paradigms workshop*. Association for Computing Machinery, New York, NY, USA, 1–15. doi:10.1145/3368860.3368861

[68] UK Parliament. 2017. Digital Economy Act 2017. https://www.legislation.gov.uk/ukpga/2017/30/contents.

[69] Payplan and Refuge. 2020. *Safe pathways into debt advice for domestic abuse survivors.* Technical Report. Payplan and Refuge.

[70] Audrey Pereira, Amber Peterman, Anastasia Naomi Neijhoft, Robert Buluma, Rocio Aznar Daban, Aminul Islam, Esmie Tamanda Vilili Kainja, Inah Fatoumata Kaloga, They Kheam, Afrooz Kaviani Johnson, et al. 2020. Disclosure, reporting and help seeking among child survivors of violence: a cross-country analysis. *BMC public health* 20 (2020), 1–23. doi:10.1186/s12889-020-09069-7

[71] Lyne Piché, Jeffrey Mathesius, Patrick Lussier, and Anton Schweighofer. 2018. Preventative services for sexual offenders. *Sexual Abuse* 30, 1 (2018), 63–81. doi:10.1177/1079063216630749

[72] Claudette Pretorius, Darragh McCashin, Naoise Kavanagh, and David Coyle. 2020. Searching for mental health: a mixed-methods study of young people's online help-seeking. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376328

[73] Lucy Qin, Vaughn Hamilton, Sharon Wang, Yigit Aydinalp, Marin Scarlett, and Elissa M. Redmiles. 2024. "Did they F***ing consent to that?": safer digital intimacy via proactive protection against image-based sexual abuse. In *Proceedings of the 33rd USENIX Conference on Security Symposium* (Philadelphia, PA, USA) *(SEC '24)*. USENIX Association, USA, Article 4, 18 pages.

[74] Alana Ray and Nicola Henry. 2025. Sextortion: A Scoping Review. *Trauma, Violence, & Abuse* 26, 1 (2025), 138–155. doi:10.1177/15248380241277271

[75] Elissa M. Redmiles, Jessica Bodford, and Lindsay Blackwell. 2019. "I Just Want to Feel Safe": A Diary Study of Safety Perceptions on Social Media. *Proceedings of the International AAAI Conference on Web and Social Media* 13, 01 (Jul. 2019), 405–416. doi:10.1609/icwsm.v13i01.3356

[76] Refuge. 2024. *Annual report and financial statements.* Technical Report. Refuge.

[77] Louise Robinson and Karen Spilsbury. 2008. Systematic review of the perceptions and experiences of accessing health services by adult victims of domestic violence. *Health & social care in the community* 16, 1 (2008), 16–30. doi:10.1111/j.1365-2524.2007.00721.x

[78] Joni Salminen, Kathleen Wenyun Guan, Soon-Gyo Jung, and Bernard Jansen. 2022. Use cases for design personas: A systematic review and new frontiers. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–21. doi:10.1145/3491102.3517589

[79] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. " They Don't Leave Us Alone Anywhere We Go" Gender and Digital Abuse in South Asia. In *proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3290605.3300232

[80] Morgan Klaus Scheuerman, Stacy M. Branham, and Foad Hamidi. 2018. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 155 (Nov. 2018), 27 pages. doi:10.1145/3274424

[81] Carol F Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W Newman, and Sarita Schoenebeck. 2023. Trauma-Informed Social Media: Towards Solutions for Reducing and Healing Online Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 341, 20 pages. doi:10.1145/3544548.3581512

[82] Nicola Sharp-Jeffs and Liz Kelly. 2016. *Domestic homicide review (DHR): Case analysis.* Technical Report. Standing Together Against Domestic Violence.

[83] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3290605.3300319

[84] Julia Slupska and Angelika Strohmayer. 2022. Networks of Care: Tech Abuse Advocates' Digital Security Practices. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 341–358. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks

[85] Julia Slupska and Leonie Maria Tanczer. 2021. Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things. In *The Emerald international handbook of technology-facilitated violence and abuse*. Emerald Publishing Limited, 663–688. doi:10.1108/978-1-83982-848-520211049

[86] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse. In *32nd USENIX Security Symposium*

(USENIX Security 23). USENIX Association, Anaheim, CA, 69–86. https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-vectors

[87] Isabel Straw and Leonie Tanczer. 2023. 325 Digital technologies and emerging harms: identifying the risks of technology-facilitated abuse on young people in clinical settings. *Archives of Disease in Childhood* 108, Suppl 2 (2023), A54–A54. doi:10.1136/archdischild-2023-rcpch.91

[88] Sharifa Sultana, Mitrasree Deb, Ananya Bhattacharjee, Shaid Hasan, S.M.Raihanul Alam, Trishna Chakraborty, Prianka Roy, Samira Fairuz Ahmed, Aparna Moitra, M Ashraful Amin, A.K.M. Najmul Islam, and Syed Ishtiaque Ahmed. 2021. 'Unmochon': A Tool to Combat Online Sexual Harassment over Facebook Messenger. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 707, 18 pages. doi:10.1145/3411764.3445154

[89] Takuro Suzuki. 2024. A survey on the reasons why victims of stalking did not exhibit help-seeking behavior: a text-mining analysis. *BMC psychology* 12, 1 (2024), 515. doi:10.1186/s40359-024-02035-7

[90] Leonie Maria Tanczer, Isabel López-Neira, and Simon Parkin. 2021. 'i feel like we're really behind the game': perspectives of the united kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of gender-based violence* 5, 3 (2021), 431–450. doi:10.1332/239868

[91] Leonie Maria Tanczer, Ine Steenmans, Miles Elsden, Jason Blackstock, and Madeline Carr. 2018. Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. IEEE, 1–9. doi:10.1049/cp.2018.0033

[92] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, et al. 2021. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 247–267. doi:10.1109/SP40001.2021.00028

[93] Emily Tseng, Rosanna Bellini, Yeuk-Yu Lee, Alana Ramjit, Thomas Ristenpart, and Nicola Dell. 2024. Data Stewardship in Clinical Computer Security: Balancing Benefit and Burden in Participatory Systems. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 39 (April 2024), 29 pages. doi:10.1145/3637316

[94] 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)*. USENIX Association, 1893–1909. https://www.usenix.org/conference/usenixsecurity20/presentation/tseng

[95] 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* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 71, 17 pages. doi:10.1145/3411764.3445589

[96] 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 *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–20. doi:10.1145/3491102.3502038

[97] Kieron Ivy Turk and Alice Hutchings. 2023. Click Here to Exit: An Evaluation of Quick Exit Buttons. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 547, 15 pages. doi:10.1145/3544548.3581078

[98] Willem G Van Panhuis, Proma Paul, Claudia Emerson, John Grefenstette, Richard Wilder, Abraham J Herbst, David Heymann, and Donald S Burke. 2014. A systematic review of barriers to data sharing in public health. *BMC public health* 14 (2014), 1–9. doi:10.1186/1471-2458-14-1144

[99] Emily A. Vogels. 2021. *The State of Online Harassment*. Technical Report. Pew Research Center.

[100] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2344–2360. doi:10.1109/SP46214.2022.9833643

[101] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Tara Matthews, Sarah Meiklejohn, Franziska Roesner, Renee Shelby, Kurt Thomas, and Rebecca Umbach. 2024. Understanding Help-Seeking and Help-Giving on Social Media for Image-Based Sexual Abuse. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4391–4408. https://www.usenix.org/conference/usenixsecurity24/presentation/wei-miranda-understanding

[102] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Franziska Roesner, and Kurt Thomas. 2023. "There's so much responsibility on users right now:" Expert Advice for Staying Safer From Hate and Harassment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 190, 17 pages. doi:10.1145/3544548.3581229

[103] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M. Redmiles, and Franziska Roesner. 2024. SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 7011–7030. https://www.usenix.org/conference/usenixsecurity24/presentation/wei-miranda-solk

[104] Katherine R White and Donald G Dutton. 2012. Perceptions of female perpetrators. In *Perceptions of female offenders: How stereotypes and social norms affect criminal justice responses*. Springer, New York, USA, 101–116. doi:10.1007/978-1-4614-5871-5

[105] Jenna M Wilson and Kimberly Smirles. 2022. College students' perceptions of intimate partner violence: The effects of type of abuse and perpetrator gender. *Journal of interpersonal violence* 37, 1-2 (2022), 172–194. doi:10.1177/0886260520908025

[106] UN Women. 2024. *ADDRESSING GAPS TO PREVENT AND ELIMINATE TECHNOLOGY-FACILITATED (TF) GENDER-BASED VIOLENCE AGAINST WOMEN AND GIRLS*. Technical Report. UN Women.

[107] Delanie Woodlock, Karen Bentley, Darcee Schulze, Natasha Mahoney, Donna Chung, and Amy Pracilio. 2020. *Second national survey of technology abuse and domestic violence in Australia*. Technical Report. WESNET.

[108] Jessica Woolley, Mary Iliadis, and Marilyn McMahon. 2023. Digital coercive control: barriers to victim/survivors' help-seeking and risk management in Victoria. *Journal of Gender-Based Violence* 7, 3 (2023), 383–398. doi:10.1332/239868021X16891521203616

[109] Elizabeth Yardley. 2021. Technology-facilitated domestic abuse in political economy: A new theoretical framework. *Violence against women* 27, 10 (2021), 1479–1498. doi:10.1177/1077801220947172

[110] Wenqi Zheng, Emma Walquist, Isha Datey, Xiangyu Zhou, Kelly Berishaj, Melissa Mcdonald, Michele Parkhill, Dongxiao Zhu, and Douglas Zytko. 2024. "It's Not What We Were Trying to Get At, but I Think Maybe It Should Be": Learning How to Do Trauma-Informed Design with a Data Donation Platform for Online Dating Sexual Violence. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 743, 15 pages. doi:10.1145/3613904.3642045

[111] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 429–446. https://www.usenix.org/conference/usenixsecurity21/presentation/zou

A Step-by-step process of *Refuge*'s victim/survivor support

Here, we highlight the step-by-step process a victim/survivor goes through when they approach or are referred to *Refuge* for support. Firstly, they typically reach out to *Refuge* via the helpline, local outreach services, or they are referred by a professional. This can include the police, healthcare professionals, or children's services etc. They share their lived experience with a front-line specialist who gathers demographic details and records key points. This is followed by a technology assessment that ensures the victim/survivor's safety regarding app and device settings.

Next, a standardised Domestic Abuse, Stalking, and 'Honour'-based Abuse (DASH) risk assessment is carried out, alongside a *Refuge*-specific questionnaire unique to the service's process and data management system, which can not be disclosed for confidentiality and intellectual property reasons. A section of this assessment is dedicated to the victim/survivor's experience of tech abuse.

Based on the assessment, a safety plan of agreed-upon actions is discussed with the victim/survivor. This leads to one of three outcomes: (1) support within the community, (2) admission to a refuge, or (3) the woman declines support. Community support is provided to women who do not require or wish to access accommodation at one of *Refuge*'s domestic abuse shelters (also commonly referred to as a "refuge"). Instead, they work with an outreach support worker who meets with them in their home or another safe place. For these victim/survivors, an initial check that their phone is secure and that it is safe to communicate occurs before their DASH risk assessment. The more thorough tech assessment is then conducted after. Victim/survivors admitted to a refuge or safe house stay as long as necessary and work with an allocated key worker to secure permanent housing. Upon leaving *Refuge*'s service, an exit questionnaire is conducted to assess their situation. The data analysed in this study includes both the initial risk assessment and the exit questionnaire.

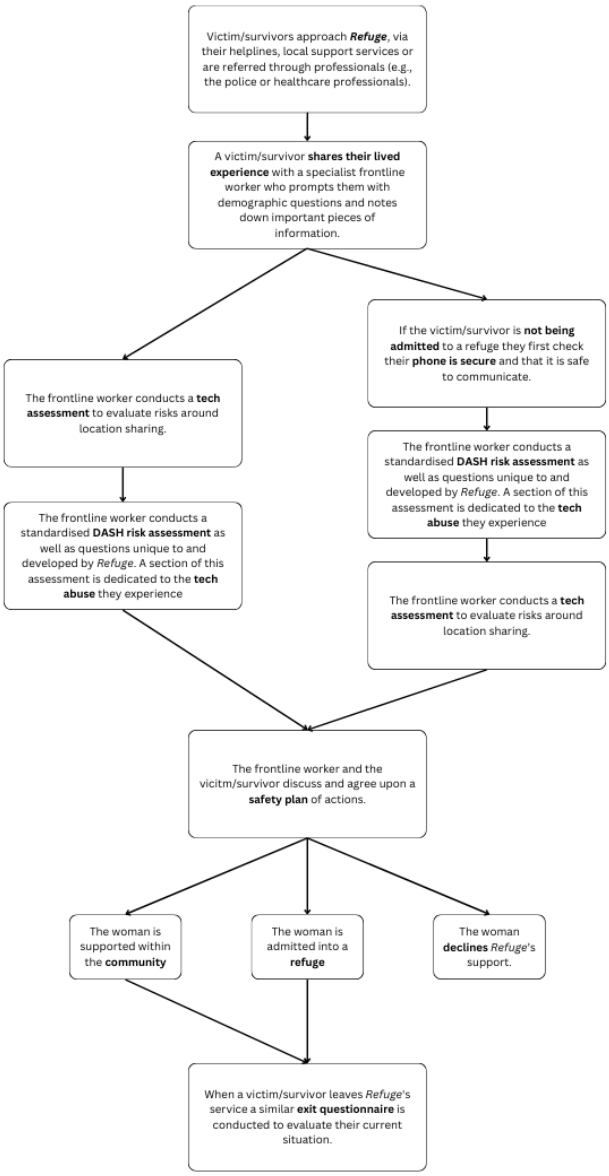

Figure 1: Flowchart depicting *Refuge*'s process. The data analysed here comes from the risk assessment and exit questionnaire.

B Graphical representation of the seven personas, their tech abuse experiences, and their unique help-seeking behaviours

The graphic below showcases all seven personas identified from this dataset of real victim/survivors. It highlights their defining attribute, the types of tech abuse they experienced, and the help-seeking behaviours they showcased. They also indicate the percentages of each persona that experienced physical, sexual, psychological, and financial abuse as well as the percentages that had sought help before.

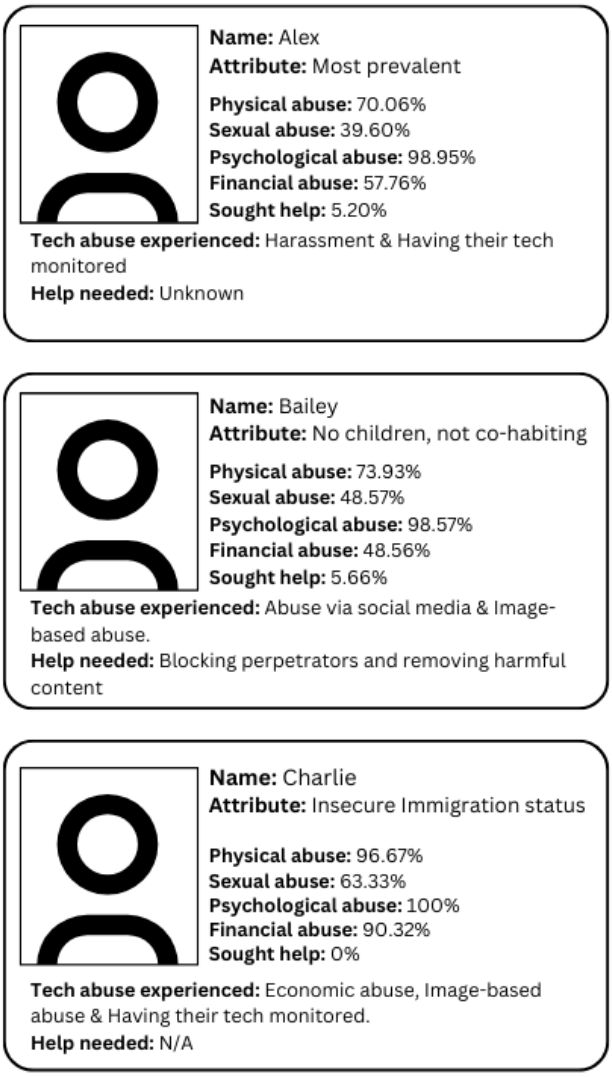

Figure 2a: Characteristics of Personas A-C, their abuse, and help-seeking experiences.

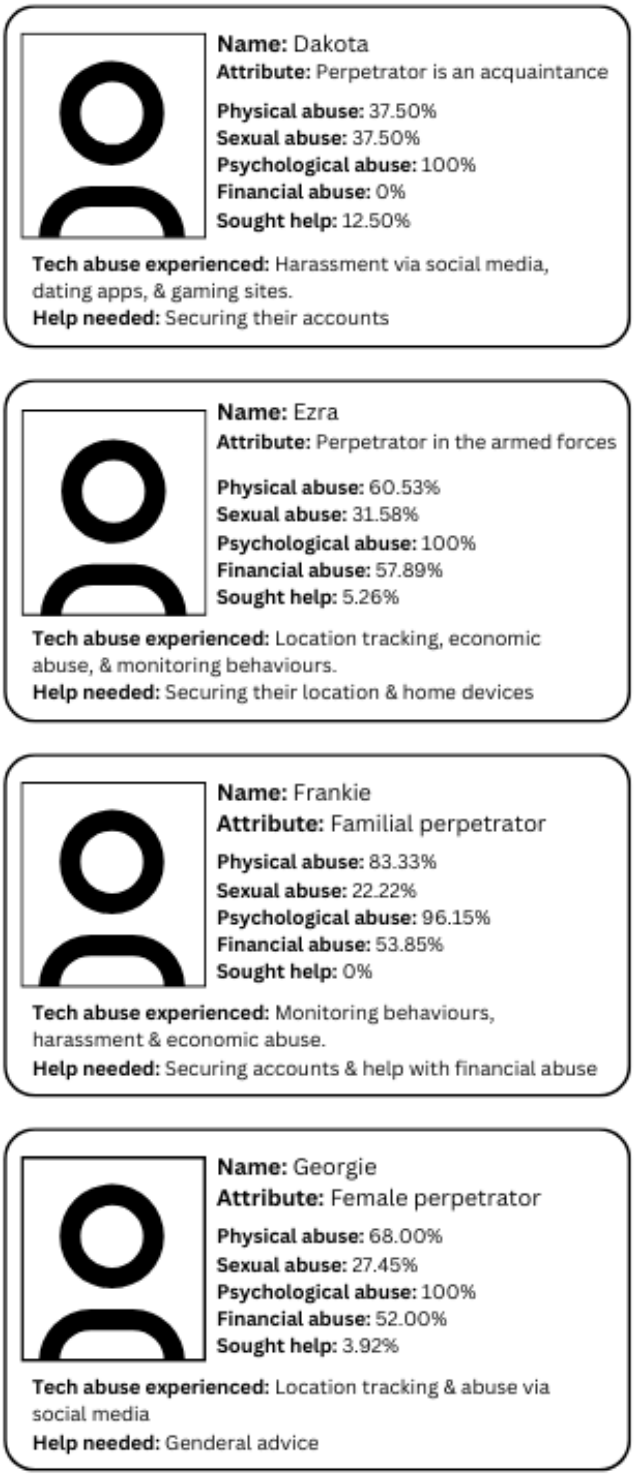

Figure 2b: Characteristics of Personas D-G, their abuse, and help-seeking experiences.