Journal of Gender-Based Violence • vol XX • no XX • 1–20 • © Centre for Gender and Violence Research
University of Bristol 2021 • Print ISSN 2398-6808 • Online ISSN 2398-6816
https://doi.org/10.1332/239868021X16290304343529

article

'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

Leonie Maria Tanczer, l.tanczer@ucl.ac.uk
Isabel López -Neira, x.lopez-neira.17@alumni.ucl.ac.uk
University College London

Simon Parkin, s.parkin@ucl.ac.uk
Delft University of Technology, previously University College London

Technology-facilitated abuse or 'tech abuse' in intimate partner violence (IPV) contexts describes the breadth of harms that can be enacted using digital systems and online tools. While the misappropriation of technologies in the context of IPV has been subject to prior research, a dedicated study on the United Kingdom's IPV support sector has so far been missing. The present analysis summarises insights derived from semi-structured interviews with 34 UK voluntary and statutory sector representatives that were conducted over the course of two years (2018–2020). The analysis identifies four overarching themes that point out support services' practices, concerns and challenges in relation to tech abuse, and specifically the Internet of Things (IoT). These themes include (a) technology-facilitated abuse, where interviewees outline their experiences and understanding of the concept of tech abuse; (b) IoT-enabled tech abuse, focusing on the changing dynamics of tech abuse due to the continuing rise of smart consumer products; (c) data, documentation and assessment, that directs our attention to the shortcomings of existing risk assessment and recording practices; and (d) training, support and assistance, in which participants point to the need for specialist support capabilities to be developed within and beyond existing services.

Key words technology-facilitated abuse • technology-mediated abuse • technology-enabled abuse • tech abuse • Internet of Things

Key messages

- UK statutory and voluntary support services do not feel well equipped to respond to tech abuse.
- Shortcomings in documentation and assessment practices make it difficult to estimate the full scale and nature of tech abuse.
- Tech abuse training and other support mechanisms are needed to amplify the UK sector's ability to assist IPV victims/survivors.

To cite this article: Tanczer, L. Parkin, S. and López -Neira, I. (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*, vol XX, no XX, 1–20, DOI: 10.1332/239868021X16290304343529

Introduction

Technology-facilitated abuse or 'tech abuse' describes the breadth of harms that can be enacted using digital systems and online tools, including smartphones, GPS-trackers and internet-enabled products. To date, tech abuse is a rather ambiguous concept. The term is contested (Dragiewicz et al, 2018; Markwick et al, 2019) and other notions such as 'ICT-facilitated violence' (UN Women, 2020), 'technology-mediated abuse' (Eckstein, 2020), or 'technology-based abuse' (Messing et al, 2020) exist. However, tech abuse generally pinpoints towards technologies' intermediate role in intimate partner violence (IPV) situations. Its manifestation ranges from the distribution of intimate images without a person's consent ('revenge porn'), the harassment of an individual such as seen in the context of cyberstalking, to the impersonation of affected parties. Tech abuse further stretches from 'simple' and technologically 'unsophisticated' attacks such as excessive text messaging, to more elaborate actions including the circumvention of privacy and security measures and the compromise of a device with malicious software ('spyware'). Most commonly, tech abuse scenarios involve a 'UI-bound adversary'. The latter describes an actor that misuses existing device interfaces, pre-existing functionalities and ready-made application rather than malicious or sophisticated software tools (Freed et al, 2018).

The misappropriation of digital technologies in the context of IPV has been subject to prior research. Scholars such as Woodlock (2017), Douglas et al (2019), Matthews et al (2017), and Freed et al (2017) studied the role and experiences the misuse of technologies for IPV victims/survivors creates. While digital systems offer opportunities to assist IPV victims/survivors (Arief et al, 2014; Burdon and Douglas, 2017; Rodríguez-Rodríguez et al, 2020) and to challenge perpetrator's behaviours (Bellini et al, 2020), the exploitation of technologies to harm, monitor and dominate victims/survivors can be positioned within Kelly's conceptualisation (1988) of a 'continuum of violence' (Harris, 2020). Thus, offline and online abuse forms closely intersect and overlap with other coercive and controlling behaviours (Stark, 2007; 2016; Stark and Hester, 2019).

Besides, tech abuse is perceived as a dominantly gendered phenomenon (Henry and Powell, 2016). While research identified that women and men generally report experiencing a similar scale of tech abuse victimisation, the nature and impacts of those experiences differ (Powell and Henry, 2019). Thus, women are significantly more likely than men to consider their exposure to digital sexual harassment and other forms of online sexual victimisation as moderately to extremely upsetting and are more likely to feel negative impacts as a result of their victimisation. Yardly (2020), therefore, speaks of tech abuse as a neoliberal manifestation of patriarchal power structures, which further needs to be contextualised alongside different geographical and cultural settings (Sambasivan et al, 2019).

The increasing attention on tech abuse is of importance as digital technologies evolve. Specifically, the rise of the so-called Internet of Things (IoT) is hereby noteworthy. IoT describes a pivotal move away from 'conventional', internet-connected devices such as smartphones and laptops towards a far more interdependent ecosystem of different interconnected products and services. IoT is consequently 'the direct and indirect extension of the internet into a range of physical objects' (Tanczer et al, 2019a: 37). While many devices were previously 'offline' and 'analogue', they have now – due to their upsurge in functionality and connectivity – become 'smart'. One can consequently speak of 'smart' household appliances such as TVs, cameras or doorbells that can be remotely controlled, have audio and video recording functionalities, and collect reams of personal information. Examples of popular IoT systems are smart speakers such as Amazon Echo or Google Home, internet-connected doorlocks such as the August Smart Lock, and temperature control devices such as the Nest thermostat.

IoT is further characterised by a shift away from personal, individually owned towards collectively, shared devices. This transition creates novel privacy and security risks that demand new safety and security requirements (Slupska and Tanczer, 2021; Tanczer, 2021). In contrast to other technologies such as the smartphone or social media applications, the impact IoT devices create for IPV victims/survivors has been less widely studied. One of the earliest research projects examining this issue has been the 'Gender and IoT' (GIoT) pilot study at University College London (Tanczer et al, 2018b). From the beginning of 2018 onwards, the GIoT research team has co-developed their work with the UK's support sector to assess IoT's role and its unique IPV risk trajectories (Lopez-Neira et al, 2019; Parkin et al, 2019). The group has also been engaged in advising ongoing policy debates around domestic abuse, online harms, as well as IoT security (Tanczer, 2019; Tanczer et al, 2019b; 2018a) and conducted tech abuse training sessions such as a dedicated 'CryptoParty' for representatives of the UK support sector (UCL STEaPP, 2018).

More recently, scholars such as Leitão (2019), Slupska (2019) and Janes et al (2020) have added to this burgeoning, IoT-specific literature and helped to uncover why in-home privacy security threats deriving from smart systems require closer attention. For instance, in many cases the usability of smart devices is limited due to the restricted user interface that is available, and proposed security and privacy recommendations often conflict with each other when examined across the three different abuse phases (that is, physical control, escape, life apart) (Matthews et al, 2017; Parkin et al, 2019; Alshehri et al, 2020). Besides, devices often suffer from flaws that enable unauthorised access, with such a deficiency of transparency endangering particularly vulnerable groups and communities (Janes et al, 2020). In addition, researchers exposed a lack of awareness on IoT-facilitated tech abuse across support services such as voluntary sector organisations like refuges and charities, and statutory service bodies such as law enforcement (Tanczer et al, 2018b; Mayhew and Jahankhani, 2020), which limits the support affected victims/survivors can expect.

The present study

Drawing on this previous body of work, the present study focuses in on the privacy and security risks that IoT systems create while providing a broader analysis of the

perceived state of tech abuse preparedness among representatives of the UK's IPV statutory and voluntary support sector. Based on qualitative interviews conducted over the course of two years, the upcoming analysis identifies four overarching themes that offer insights into the support services' practices, concerns and challenges in relation to tech abuse, and specifically IoT. The analysis highlights the increasing demand for the provision of specialist support that frequently necessitates technical awareness and expertise. The latter will be even more urgently needed as digital technologies become more enshrined in everyday life, and IoT's usage increases. The results further uncover the value of having a dedicated concept for referring to technology-mediated abuse forms, better means to collate, document and assess tech abuse-related incidents, and dedicated training and support mechanisms available. The study is part of the broader activities of the GIoT research team, to which the authors are affiliated, and sets important pointers for future research, policy developments and efforts to bolster the support sector's practices.

Method

Participants and data collection

We interviewed a self-selected sample of 34 representatives from the UK voluntary (n=28) and statutory (n=6) support sector between May 2018 and July 2020. Participants came primarily from England, with a few interviewees based in Wales and Scotland, and none from Northern Ireland. They were both from first- as well as second-tier organisations and held a range of positions, including frontline roles such as Independent Domestic Violence Advisors (IDVA) or detectives as well as managerial roles such as directors or coordinators. Following the receipt of ethical approval (Project ID Number: 10503/001), we enlisted participants through recruitment emails sent to support services, members of the London VAWG Consortium (a coalition of specialist VAWG providers), and personal contacts. Additional participants were recruited using snowball sampling. All semi-structured interviews were conducted by the first author using the telephone or Voice over Internet Protocol services such as Microsoft Teams or Zoom, and were part of a wider research engagement organised by the research team (for example, co-development workshops, tech abuse training). As seen in Table 1, interviews lasted commonly between 30 and 60 minutes, with our interview outline covering issues such as the frequency and nature of tech abuse, assessment and documentation practices, as well as tech abuse resources, concerns and support needs (Appendix A). All interviews were audio-recorded, transcribed and then anonymised.

Data analysis

We evaluated the interviews using a deductive approach to thematic analysis (Braun and Clarke, 2006), with themes discussed in this article deriving from the interview outline and its structure. Each member of the research team participated in the code creation. After that, we discussed and agreed on the four final themes. The lead author had the final overview of the codebook creation. The following section features interview extracts. Participants are referred to as 'P' plus identifying number (that is, P1). The symbol '(…)' is used to identify negligible sections of an interview.

Table 1: Overview of interviewees

Participant	Sector	Date	Length	Participant	Sector	Date	Length
P1	VS	May 2018	47min	**P18**	VS	June 2020	46min
P2	VS	May 2018	35min	**P19***	VS	June 2020	97min
P3	VS	May 2018	32min	**P20**	VS	June 2020	24min
P4	VS	May 2018	50min	**P21**	VS	June 2020	28min
P5	VS	August 2018	67min	**P22**	VS	June 2020	48min
P6	SS	September 2018	39min	**P23**	VS*	June 2020	44min
P7	VS	October 2018	42min	**P24**	VS	June 2020	34min
P8	SS	October 2018	55min	**P25**	VS	June 2020	30min
P9	SS	September 2018	73min	**P26**	VS	June 2020	38min
P10	VS	January 2019	35min	**P27**	SS	July 2020	57min
P11	VS	January 2019	29min	**P28**	VS	July 2020	42min
P12	SS	February 2019	48min	**P29**	VS	July 2020	39min
P13	VS	February 2019	31min	**P30**	VS	July 2020	42min
P14	VS	March 2019	36min	**P31**	SS	July 2020	47min
P15	VS	June 2019	50min	**P32**	VS	July 2020	32min
P16	VS	June 2020	39min	**P33**	VS	July 2020	29min
P17	VS	June 2020	38min	**P34**	VS	July 2020	36min

Note VS: Voluntary Sector; SS: Statutory Sector; VS:* organisation that specialises on cybersecurity and work with IPV victims/survivors in a secondary function.

Results

The analysis focuses on the perspectives of the UK's IPV sector towards tech abuse. All interviews raise important questions about the UK's level of preparedness when it comes to this evolving phenomenon. Participants point to the diverse patterns that fall under the remit of tech abuse and highlight the need for better assessment, documentation and reporting practices. Interviewees frequently stress that more needs to be done to support them in their assistance of tech abuse victims/survivors. Moreover, throughout our data collection process from 2018 to 2020, interviewees expressed increasing awareness and exposure to new and emerging forms of tech abuse, including through smart, internet-connected devices. This showcases a possible transformation and expansion that tech abuse is undergoing and describes responsive and proactive efforts to tackle the challenges from within the sector. To exhibit some of the most prominent arguments that underpinned our conversations with sector representatives, we discerned four distinct themes. These themes are (a) technology-facilitated abuse, where interviewees outline their experiences and understanding of the concept of tech abuse; (b) IoT-enabled tech abuse, focusing on the changing dynamics of tech abuse due to the continuing rise of smart consumer products; (c) Data, documentation and assessment, that directs our attention to the shortcomings of existing risk assessment and recording practices; and (d) Training, support and assistance, in which participants point to the need for specialist support capabilities to be developed within and beyond existing services. All themes are now outlined here and thereafter discussed considering the current state of the literature and evidence base.

Technology-facilitated abuse

The first theme offers an overview of participants' viewpoints on the notion of tech abuse and its corresponding connotations. Generally, tech abuse is associated with the deliberate misuse of digital forms of technologies for monitoring, 'tracking' (P4, P15), and controlling victims/survivors. For interviewees, tech abuse has become 'part of the abuse portfolio' (P21). It is related to existing offences such as 'stalking' (P6, P7, P16, P31), 'harassment' (P5, P9, P22, P29, P34), and 'coercive control' (P14, P17, P29) and thought of as widespread and 'quite common' (P34). While most UK support service representatives were not able to offer 'a quantitative figure' (P3) on the scale of tech abuse, interviewees highlighted that 'in all cases of domestic abuse, I would expect there to be an aspect of online abuse and surveillance' (P18). This is because tech abuse 'comes up' (P24) 'with pretty much every victim that comes through' (P26) their service.

Outlined tech abuse dynamics stretch from low-tech (that is, simplistic attack scenarios) to more sophisticated abuse forms. On one side of the spectrum are instances that involve 'just' (P25) 'unsolicited phone calls' (P27) or the excessive and repetitive sending of messages. The latter can include text messages, emails or social media/bulletin board postings as well as images (that is, 'revenge porn'; P6, P16, P17, P28). All such communication-based tactics allow perpetrators to maintain 'unwanted contact' (P28), with smartphones being the primary 'weapon of choice' (P30).

More technical abuse dynamics include diverse forms of 'surveillance within' (P26) and outside the home. Interviewees referred to the 'cloning of phones' (P6, P22), the installation of 'keyloggers' (P15) and 'spyware' (P8, P15, P17, P33) as well as the 'bugging' (P24) of systems such as laptops and phones. Additionally, issues such as 'identify theft' (P22), 'impersonation' (P3), 'doxxing' (P16), 'iCloud hacks' (P2, P23), the creation of 'fake profiles' (P16) and the posting of 'bad reviews' (P25) on victim's/survivor's associated businesses were voiced. Indeed, some perpetrators go as far as to check 'the internet history' (P32), 'befriend other people that are connected' (P16) with the victim/survivor, or are known to have paid 'others to be hacking and finding out information about other individuals' (P14).

One interviewee spoke to the skewed perception of tech abuse which – even within the support sector – is perceived as requiring profound 'hacking' (P33) and technical skills and being 'hard' (P33) to pursue. However, in most cases, perpetrators are not required to be 'IT-savvy' (P33). Off-the-shelf surveillance products exist, and the simple 'guessing of passwords' (P25) is common enough to achieve access to victim's/survivor's accounts. Moreover, tech abuse should not be perceived as solely the malicious use of technology but also the deliberate withholding of access to digital products and services. According to interviewees, perpetrators 'will cut them [victims/survivors] off' (P14) from devices and platforms, or not allow victims/survivors 'to friend certain people' (P10). In both instances, perpetrators exert control in a way that is detrimental to the other party.

The exact scale of tech abuse 'depends to the extent that the perpetrator is willing to go to, how much resources [they have] and how deeply they are invested into somebody' (P14). Their methods are diverse, 'creative' (P27) and 'inventive' (P16). For example, instead of buying a dedicated tracker, we heard of perpetrators who 'duct-taped' (P6) mobile phones such as iPhones underneath victims'/survivors' cars or who engaged in 'one-pe-ing' (P1). The latter describes a tactic whereby the perpetrator

transfers 'one penny into the victim's bank account' (P27) with them 'leaving little messages in the transfer' (P16) note.

Indeed, tech abuse can take benign traits that only upon close inspection with other harassing strategies become lucid. As one UK support sector representative emphasised: 'some perpetrators seem to be quite clever at posting things which couldn't really be' (P28) evident as a potential breach of, for example, a non-molestation order such as 'abstract messages or photos being posted, say, like around anniversaries of breakups' (P28). This ambiguity that surrounds tech abuse becomes vividly apparent in Extract 1:

> Extract 1:
> 'perpetrator will use like mobile phones effectively to do things. Like when they know the woman's like three-quarters of the way there to drop the child off, they'll go, "Oh, actually, I can't be there now for half an hour," so they use technology to keep women actually unable to get on with their life. It's really hard to prosecute that kind of stuff.' (P28)

The quote showcases how perpetrators deliberately exploit their position of power. This dynamic is further amplified because 'they're the ones that are [frequently] more technologically-savvy' (P15) within an abusive relationship. They are often also the legal owner of a device and service contract, with male abusers having been described as 'more experienced than women' (P7) when it comes to the usage of digital systems. Interviewees stressed that perpetrators commonly 'setup' (P15) their victims'/survivors' phones or laptops. Interviewees indicate that offenders generously offer devices 'at the beginning of a relationship' (P15) which are later used to monitor and control their partners. Gifting dynamics consequently 'lay the groundwork for complete surveillance' (P19) with perpetrators deliberately taking 'control of the IT in the relationship' (P19).

IoT-enabled tech abuse

The second theme outlines participants' responses to questions related to emerging forms of tech abuse, specifically smart, internet-connected devices. While tech abuse remains 'very phone-based' (P32), IoT-facilitated tech abuse was a concept known to most interviewees. Participants had heard or experienced perpetrators misusing systems such as the smart thermostats like 'Hive' (P20, P26) and 'Nest' (P19). They also referred to Amazon's Ring 'doorbell' and 'camera' (P16, P17, P26, P30, P34), 'smart speakers' (P27) and 'home assistants' (P33) such as Amazon 'Echo' (P11, P17), internet-connected 'baby monitors' (P27), 'children's devices' (P33), and smart wearables such as the 'Fitbit' (P32).

IoT-facilitated tech abuse was not considered to be widespread, as support services would 'rarely hear' (P1) about IoT systems in their day to day practice. According to interviewees, most clients would not 'have these kind of gadgets' (P7) or perhaps 'just aren't aware that it [IoT-facilitated tech abuse] might be going on' (P33). Interviewees perceive that the deployment of IoT is yet to reach its full scale, showcased by statements such as: 'I think we're at a stage with this IoT stuff that we were a few years ago with the social media stuff' (P10). Hence, while some participants have 'never seen it [IoT-facilitated abuse] directly' (P12), there is a broader 'concern about those

devices being used inappropriately' (P4) with most having the expectation that such abuse dynamics will become more prevalent 'as we move forward and more things become connected' (P16).

Among one of the core risks that interviewees see deriving from smart devices for IPV victims/survivors are their ability to facilitate 'gaslighting' (P16). The latter concept refers to situations where a perpetrator undermines the victim's/survivor's reality by denying facts, the environment around them, or their feelings. As a consequence, the victim/survivor may start to question their sanity, perception of reality, or memories (Sweet, 2019). In our study, participants worry about the omnipresence of the perpetrator that these internet-connected devices can create, the 'illusion of protection' (P18) these devices may generate, as well as the 'camouflaged' (P18) element that many smart systems represent. Drawing on their experience of working with victims/survivors, the functionalities that IoT systems embody – such as 'turning the heating off and on and the lights' (P27) – would give abusers 'another vector' (P12) for tormenting victims/survivors. Support sector representatives, therefore 'think the impact that that [IoT] will have on people, particularly if it's happening after the breakdown of an abusive relationship, is that people will feel like they are going insane' (P16). This dynamic is described in Extract 2:

> Extract 2:
> 'they can never be free from the abuse because the person is always there, is always looking over your shoulder. When you live like that, you can never feel 100 per cent safe. You don't know who to trust, so you start potentially isolating yourself, because you don't know if this is coming from a person, or it's coming from a device (…). Abuse itself is not about just a physical presence of the perpetrator, it's the emotional, mental, manipulating, coercive, control, and this is what these devices, although we all love them when they're used in a positive manner, but it really can be used in such a negative connotation, which we have seen.' (P20)

Hence, IoT devices are perceived to affect both the perceived as well as the actual security of victims/survivors. This dynamic is further exacerbated by the fact that many technical systems have 'been set up by the perpetrator' (P16), that abusers will often 'convince someone close to a survivor that the survivor is making stuff up' (P18), and that 'it can be really hard to roll all of that access back' (P19) when victims/survivors try to extract themselves from an abusive environment. Additionally, the ambivalence between the simplicity of purchasing and setting up IoT devices versus amending user setting is a fear. For one interviewee, it is 'much harder to work out exactly how to use things safely' (P33) then continuing to use these devices in its predefined, insecure state. Such arguments point at the issue that 'not everyone is literate enough to use this system[s]' (P32). These shortcomings can exceed the potential positive elements of IoT systems, including their ability to gather 'evidence' (P12), 'communicate with other people' (P19) or offer an avenue to set off an 'alarm' (P28).

Data, documentation and assessment

The third theme explores interviewees' perception of the state of available data on tech abuse, and shortcomings in the UK support sector's documentation and

assessment practices. Participants generally referred to using existing risk assessment procedures such as the Domestic Abuse, Stalking and Harassment and Honour Based Violence (DASH) Risk Checklist, and variants such as the Screening Assessment for Stalking and Harassment (SASH). One of the main concerns about DASH was that its questions 'don't feature specifically tech abuse' (P34). While most interviewees acknowledged that they do not 'stick to' (P32) the DASH rigidly because they consider it 'a guide, rather than be the gospel' (P32), this omission would be one of DASH's blind spots. It would make the current risk assessment approach 'outdated' (P30) and 'antiquated' (P18).

Interviewees frequently lacked 'internal guidance' (P24) on how to deal with tech abuse with participants admitting that the sector should 'stress' (P2) tech abuse more in their 'day to day language' (P34) and practice. Participants from both statutory and voluntary institutions urged to make sure that tech-related questions are 'in there' (P5, P17) and 'explicitly' (P10) accounted for in IPV risk assessments. In most organisations 'there's no specific way to record' (P6), 'measur[e] and catalog[e] incidents of tech abuse' (P3). Interviewees consequently raised the idea of adding 'one' (P6) or a 'few more questions' (P4) or 'a tick-box' (P34) about tech abuse to their recording processes. Such an inclusion could be a means for frontline workers to 'be prompted' (P31) about this issue.

Nonetheless, interviewees expressed caution about such changes. They see challenges in adding too many items to an already time-consuming procedure. Further additions would make the evaluation 'impractical' (P27). At this stage, tech abuse seems far more prominent and 'ingrained' (P33) in safety planning, where many UK support organisations 'got a whole section on technology and security' (P30). Thus, they give victims/survivors' 'basic security advice, which we have around passwords, protecting browsers, location security, social media' (P10).

A very limited number of interviewee organisations account for tech abuse as a 'specific category of its own' (P28) or touch upon it when asking victims/survivors about what 'behaviours' (P33) they are experiencing. Some organisations have responded through the development of a 'cyberstalking action plan' (P19) or the creation of 'a separate [tech abuse] form to the DASH' (P9). Besides, charities such as Refuge UK were mentioned who 'have their own tech abuse unit' (P26) and a handful of police forces have formed active collaborations between, for example, their stalking and their cybercrime teams (P9, P27).

Another difficulty our participants emphasised was that relevant tech abuse information is spread across different institutions. This is due to the diverse channels that are available to report tech-related crimes. For instance, the UK 'Home Office considers those crimes to be recorded properly by, um, er, by Action Fraud, which is a central national reporting process' (P12). However, victims/survivors may choose to 'call 101' (P12) and report the incident to a local police force. Yet, local police forces not only report crime 'differently' (P9) but can respond differently. For instance, victims/survivors may experience a police officer who is 'particularly well educated' and able to assist, or an officer who treats the incident 'less seriously' (P27).

Victims/survivors may also choose to approach 'specialist organisation' (P33) such as 'the Revenge Porn Helpline' (P33) or contact cybersecurity charities such as the 'Cyber Helpline' (P16, P33) or 'Cybercare' (P2, P7). These dynamics highlight how effective support is frequently 'down to the individual practitioner' (P30) and useful information describing the scale and nature of tech abuse is spread across miscellaneous

bodies. Interviewees as such raised the idea of incorporating tech abuse 'into the crime recording figures' (P6).

Training, support and assistance

The fourth and final theme summarises participant's interest in receiving more specialised training and their longing for better levels of assistance in tackling the growing threat of tech abuse. The theme touches upon the profound worry that interviewees sense to be falling 'behind' (P1, P3, P14, P15, P17, P24, P34). They consider themselves, their service, and the whole sector to be outrun by the fast 'pace' (P31) with which technology is being developed and rolled out. This dynamic is showcased by quotes such as 'we're still catching up with this issue' (P4), 'tech's advancing quickly' (P30), or 'it's all so new' (P5), and vividly expressed in Extract 3:

> Extract 3:
> 'Um, there's a real sense that statutory services and ourselves are behind, we're behind the wave here. Um, we know there's a wave, we can't quantify the wave and we're not measuring it, um, and we know that statutory, i.e. in, in particular instances, the police, aren't responding to it or taking it forwards because we suspect they're behind the wave too. (…) I feel like we're really behind the game.' (P3)

Interviewees further emphasised that their organisations already struggle in terms of capacity, as cases are time-consuming (P18) and 'resource-draining' (P18), 'fundraising' is a constant issue (P1), and practitioners are 'busy firefighting' (P5). Specialist frontline workers must already give guidance on 'housing' (P2) or 'legal issues' (P27) with them now also being faced with the expectation to 'have knowledge on like the cyber side' (P2). The fact that there is 'no cybersecurity expertise' (P19) in most domestic abuse and stalking charities has been highlighted as a major concern. Participants fear that evolving technologies 'will make life just a lot harder for us' (P6) and critiqued that any guidance they receive gets 'out of date so quickly' (P10, P11).

While some participants would like to see the sector being 'upskilled' (P12), interviewees are also wary that we should not 'put that level of pressure on frontline workers' (P16). Both statutory and voluntary sector representatives 'don't want to be tech experts' (P16) nor should they have to be. While a basic level of understanding must be expected and most interviewees 'absorb it [tech advice] into their current work' (P10), many participants wish for external services to which they could 'recommend people' (P18). This is of particular relevance as age was raised as an additional factor undermining participants' confidence in sufficiently supporting victims/survivors. Many interviewees were upset that they had 'no idea how' (P5) certain technologies worked. They felt 'old school' (P6), held a 'fear of technology', (P10) or a 'resistance to it' (27). Indeed, one of the most common argument we heard was that participants considered themselves as not 'tech savvy' (P2, P3, P4, P5, P6, P8, P9, P22).

Despite this deep-rooted concern, participants felt a need to keep 'up to date' (P30) with technological advancements in order to sufficiently support victims/survivors and to not give them 'a false sense of confidence' (P17). When they are stuck, they are 'downloading manuals' (19), sometimes contact their 'own federations to see if

any other organisation is experiencing something similar' (P13), ask 'IT fellas who come in and look at our laptops' (P15), 'link up with the cybercrime team at the police' (P16) or reach out to 'people in the tech sector' (P18). All these examples showcase that there is profound element of 'knowing who you can go to if you need the support and information' (P16) that must further be expanded.

Nearly all participants, therefore, highlighted the relevance of the sector receiving more 'training' (P3, P10, P11, P14, P15, P20, P21, P24, P25, P26, P29, P31, P33, P34). There is a widespread ambition 'to get more specialised [tech abuse] knowledge' (P28) with interviewees seeing a usefulness in 'having us [voluntary and statutory services] all on the same page' (P11). Any training and assistance must not be about 'scaremongering' (P11) and feature 'really practical stuff' (P10) rather than a simple 'presentation' (P25). The shared information must be 'tangible' (P27), 'digestible' (P5) and communicated in a 'simple, accessible and clear' way (P5). In addition to training, interviewees see value in receiving 'regular updates on emerging technologies' (P34), having a 'checklist of things' (P2) to look out for, 'soundbites' (P11) to explain particular topics, 'support network for them to tap into' (P14) and 'worksheets' (P34) as well as 'specific advice sheets for clients' (P33).

There are also frequent requests for some form of centralised help, because there would be no 'go-to organisation' (P25) nor a 'standard place or resource that people refer to' (P10). These appeals include calls for 'centralised guidelines' (P10), a 'one-stop-shop' (P22) for frontline staff, a 24/7 'helpline' (P17, P21) for either sector representatives or victims/survivors, or a 'website that we [the sector] can direct victims to' (P14). All these ideas point to the urge to have 'one specific organisation' (P32) the whole sector could reach out to 'in terms of tech abuse' (P30), where individuals with 'an understanding of abuse' (P3) as well as 'communication skills and the cybersecurity skills' (P19) work. To achieve such a body that is not removed from the existing know-how and experiences of frontline organisations, a 'coordinated community response' (P5) is needed, which must be about establishing valuable 'connection, rather than just yet another website' (P5).

Discussion

The present analysis summarised the perspectives of 34 UK IPV sector representatives towards tech abuse. Over the course of four themes, interview quotes and extracts offer insights on the perceived level of preparedness for this evolving phenomenon. The study sheds a light onto the UK support sector's increasing demands, practices, concerns and challenges in relation to tech abuse, and specifically IoT. The analysis highlights the increasing demand for the provision of specialist tech abuse guidance that frequently necessitates technical awareness and expertise. The latter will be even more urgently needed as digital technologies' deployment further expands and diversifies, and IoT's and other emerging technologies' usage increases. The results of our qualitative study uncover the value of having a dedicated concept for referring to technology-mediated abuse forms, better means to collect, document and assess tech abuse-related incidents, and dedicated training and support mechanisms available to assist the sector with the breadth of demands frontline workers are already facing.

Returning to the first theme surfaced in our results, technology is regarded as a common factor and an evolving new vector of abuse. This perceived prevalence stands in contrast to the lack of quantitative evidence that underpins the field. Tech abuse

patterns further seem to range from 'low-tech' (including misuse of existing features) to more 'sophisticated' manipulation of personal devices. Despite these differences, the reliance on a broad and overarching category such as 'tech abuse' may limit the ability to thoroughly differentiate between different abuse methods deployed by perpetrators. Similar to the conceptual confusions around competing interpretations of the term coercive control (Walby and Towers, 2018), the boundaries and relationships between varying tech abuse tactics will have to be defined, terminologies set and agreed (Markwick et al, 2019), and measurement categories established (Messing et al, 2020). While we are not vouching to identify and list behaviours that *are* or *are not* abusive (Dragiewicz et al, 2018), we believe it is necessary to contextualise tech abuse in order for it to receive the attention it deserves and become, for example, a dedicated category in counting rules for recorded crime laid out by the UK Home Office.

Considering our second theme, there was a sense of IoT-facilitated tech abuse not being widespread at present, but that this situation could change over time. Interviewees further expressed concern about smart devices ability to strengthen and extend a perpetrator's ability to monitor, coerce and control with these apprehensions being directly linked to the functionalities that these systems – by default – offer (Parkin et al, 2019; Janes et al, 2020). The inherent pervasiveness of such emerging technologies impacts both the perceived as well as the actual safety, security and privacy of victims/survivors. As society is only at the brink of the extensive roll-out of these systems, there is an added layer or risk that abusers deliberately exaggerate or even undersell the capabilities of technical systems. In light of the challenges such distorted viewpoints can create, it is important that measures are taken to increase the level of awareness and knowledge among users who once well-informed are better able to assess risks and to implement measures to defend against them (Harbers et al, 2018).

The third theme showcases how existing assessments (and to a lesser extent safety practices) are perceived to require further amendments to account for the risks of digital technologies. This perspective adds to prior criticism of possible omissions in standardised tools (Robinson et al, 2016; O'Shea et al, 2019) and calls for more needs-led approaches (Women's Aid, 2020). While interviewees often welcomed modifications to, for example, the DASH or their respective service's recording practices, there were concerns that additional items including tick boxes would further complicate the evaluation process. However, some participants did emphasise that add-ons such as 'cyberstalking action plan[s]' (P19) or the creation of 'a separate [tech abuse] form' (P9) are already emerging. Such efforts may spread across the sector and lead to a more nuanced evidence-base on tech abuse, which so far is scattered across different organisations and databases.

Our final theme identified the UK support sector's need to keep up with technological advances, albeit while also addressing cases as they come in. This is compounded by a seeming lack of being able to transfer experience from one application and device type to the next. The latter explains why participants feel frustrated by any guidance getting 'out of date so quickly' (P10, P11) and the constant race to hold 'pace' (P31) with technological progress. This problem seems to be further exacerbated by the increasing diversification of systems and platforms which is driven by the expansion of IoT (Carr and Tanczer, 2018). Smart, internet-connected devices currently lack standardisation (Brass et al, 2018; Tanczer et al, 2018a) and their manifold use-cases in the home, workplace and beyond create challenges to formulating generic

advice and instructions. This dynamic further feeds into the sector's sense of remaining 'behind' (P1, P3, P14, P15, P17, P24, P34). Yet, participants are conscious that the necessary technical expertise exists. However, they feel removed from this knowledge and stress that they would benefit from a more joined-up approach which may also include more centralised tech abuse efforts.

Overall, the experiences of our participants in addressing tech abuse are indicative of the increasing role technology plays in the context of IPV. Technology as 'a new tool (P5) and a 'new way of' (P5) abuse is widely considered to remain here to stay. While the tactics of tech abuse are themselves not *overly different* from previous offline/in-person abuse forms and the distress and intimidation it creates are *just as real*, technology – and especially IoT – opens numerous, remote and accessible means to monitor and control victims/survivors. Tech abuse consequently both contributes to, as much as it enlarges, our understanding of what abuse is. It, thus, deserves the same level of attention and consideration when it comes to the juridical and police response that is offered to affected parties in established abuse contexts (that is, sexual violence, financial exploitation).

Studies such as this one are, therefore, needed to unpack the increased repertoire available to perpetrators as well as the existing shortcomings and strengths which the IPV support sector is facing. Additional knowledge of the practices of 'UI-bound' abusers (Freed et al, 2018) must be put in context alongside the skewed overestimation of technical capabilities frequently perceived by frontline workers (Burton et al, 2021). There is also a clear necessity to respond to the fear of practitioners' professed lack of tech-savviness. This is especially important as IoT devices become more ubiquitous because it can cause the articulated 'distance' between the sector and technological advancement to widen further. Yet, while advocates and organisations may feel outrun by these developments, it must be emphasised that they already have the required skills to support victim's/survivor's experience of fear, confusion and disempowerment – whatever abuse form they may be exposed to.

Limitations

Our work has limitations. The self-selection sampling process was restricted in several ways, including our ability to reach support sector representatives from across the UK. First, our sample is heavily biased towards England, with only a few interviewees based in Wales and Scotland, and none from Northern Ireland. Second, our sample may have resulted in stakeholders who were less aware of tech abuse declining our invitation because of embarrassment or lack of recognition of the significance of the issue. Besides, given the qualitative research approach, caution must be taken to not generalise our findings too widely. However, we see our work as a springboard for further analyses, some of which we have already started (for example, a self-administered questionnaire, secondary data analysis of the support sector's database records).

Future work

Future research will continue the vital activity of engaging with frontline workers to understand how practitioners interact with victims/survivors on this issue and uncover the sensitivities of gathering information on this evolving phenomenon.

The capacity to prevent, mitigate and intervene in the occurrence of tech abuse is intertwined with the need to be able to effectively measure tech abuse, and be able to differentiate between tech abuse in varying levels of technical sophistication. Existing data (as collected by police and support services) must urgently be analysed, to map the scale and nature of tech abuse and identify gaps in data.

Forthcoming work can also explore the capacity to disentangle technical connections and controls that frequently assume individual rather than shared product ownership of technology and expect that users would have full access (both physically and digitally) to all its features. However, this dynamic hides the gendered dimension of tech possession and this novel form of abuse. The social and technical aspects underpinning tech abuse must therefore be closely studied, as well as the role of children and other family members, whose 'smart' or 'not-so-smart' devices may unwittingly be exploited.

Funding

The UCL 'Gender and IoT' (GIoT) project received grants from the UCL Social Science Plus+ scheme, UCL Public Policy, the PETRAS IoT Research Hub, the NEXTLEAP Project (EU Horizon 2020 Framework Programme for Research and Innovation, H2020-ICT-2015, ICT-10–2015, grant agreement No. 688722), the UK Home Office and is part of the UKRI-funded Violence, Abuse and Mental Health Network (VAMHN). Portions of work pursued by Dr Simon Parkin were completed while employed at UCL.

Acknowledgements

The authors would like to thank all interviewees for their time and interest in our study, all attendees of our prior engagement workshops and other GIoT activities, as well as many supportive colleagues – both in academia and beyond – who have helped shape our research over the past three years. Specific thanks go to Dr Trupti Patel and Professor George Danezis as well as the UCL Policy Impact Unit, including Jenny Bird and Florence Greatrix.

Conflict of interest

The authors declare that there is no conflict of interest.

References

Alshehri, A., Salem, M.B. and Ding, L. (2020) Are smart home devices abandoning IPV victims?, arXiv:2008.06612 8.

Arief, B., Coopamootoo, K.P.L., Emms, M. and van Moorsel, A. (2014) *Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse*, in Proceedings of the 13th Workshop on Privacy in the Electronic Society, WPES '14, New York: Association for Computing Machinery (ACM), pp 201–04. doi: 10.1145/2665943.2665965

Bellini, R., Forrest, S., Westmarland, N., Jackson, D. and Smeddinck, J.D. (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, Presented at the CHI '20: CHI Conference on Human Factors in Computing Systems, Honolulu, HI: Association for Computing Machinery (ACM), pp 1–14. doi: 10.1145/3313831.3376386

Brass, I., Tanczer, L.M., Carr, M., Elsden, M. and Blackstock, J. (2018) *Standardising a Moving Target: The Development and Evolution of IoT Security Standards, Presented at the Living in the Internet of Things: Cybersecurity of the IoT – 2018, IET [the Institution of Engineering and Technology]*, London. doi: 10.1049/cp.2018.0024

Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology, *Qualitative Research in Psychology*, 3(2): 77–101. doi: 10.1191/1478088706qp063oa

Burdon, M. and Douglas, H. (2017) The smart home could worsen domestic abuse. But the same technology may also make us safer, *The Conversation*, http://theconversation.com/the-smart-home-could-worsen-domestic-abuse-but-the-same-technology-may-also-make-us-safer-82897.

Burton, S., Tanczer, L.M., Vasudevan, S. and Carr, M. (2021) *The UK Code of Practice for Consumer IoT Cybersecurity: Where We Are and What Next*, London: Department of Digital Culture, Media and Sport, The PETRAS National Centre of Excellence for IoT Systems Cybersecurity.

Carr, M. and Tanczer, L.M. (2018) UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions, *Journal of Cyber Policy*, 3(3): 430–44. doi: 10.1080/23738871.2018.1550523

Douglas, H., Harris, B.A. and Dragiewicz, M. (2019) Technology-facilitated domestic and family violence: women's experiences, *The British Journal of Criminology*. 59(3): 551–70. doi: 10.1093/bjc/azy068

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N.P., Woodlock, D. and Harris, B. (2018) Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms, *Feminist Media Studies*, 18(4): 609–25. doi: 10.1080/14680777.2018.1447341

Eckstein, J.J. (2020) What is violence now? A grounded theory approach to conceptualizing technology-mediated abuse (TMA) as spatial and participatory, *The Electronic Journal of Communication* 29(3-4). Retrieved from https://www.cios.org/getfile/0290344_EJC

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. (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, New York: Association for Computing Machinery (ACM), pp 1–13. doi: 10.1145/3173574.3174241

Freed, D., Palmer, J., Minchala, D.E., Levy, K., Ristenpart, T. and Dell, N. (2017) Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders, Proceedings of the Association for Computing Machinery (ACM) on Human-Computer Interaction. 1(CSCW): 1–22. doi: 10.1145/3134681

Harbers, M., Bargh, M.S., Pool, R., Berkel, J.V., Braak, S.W.van den and Choenni, S. (2018) *A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges*, in HICSS. Presented at the 51st Hawaii International Conference on System Sciences, AIS Electronic Library, Hilton Waikoloa Village, Hawaii, pp 2215–24. doi: 10.24251/hicss.2018.278

Harris, B.A. (2020) Technology and violence against women, in S. Walklate, K. Fitz-Gibbon, J. Maher and J. McCulloch (eds) *The Emerald Handbook of Feminism, Criminology and Social Change, Emerald Studies in Criminology, Feminism and Social Change*, Melbourne: Emerald Publishing Limited, pp 317–36. doi: 10.1108/978-1-78769-955-720201026.

Henry, N. and Powell, A. (2016) Sexual violence in the digital age: the scope and limits of criminal law, *Social & Legal Studies*, 25(4): 397–418. doi: 10.1177/0964663915624273

Janes, B., Crawford, H. and OConnor, T. (2020) Never ending story: authentication and access control design flaws in shared IoT devices, in *IEEE Security and Privacy SafeThings Workshop*, San Francisco, CA: Presented at the SafeThings 2020, IEEE, pp 6.

Kelly, L. (1988) *Surviving Sexual Violence*, Cambridge: Polity Press.

Leitão, R. (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. Presented at the DIS'19, Association for Computing Machinery (ACM), San Diego, CA, pp 527–39. doi: 10.1145/3322276.3322366

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G. and Tanczer, L.M. (2019) 'Internet of Things': how abuse is getting smarter, *Safe – The Domestic Abuse Quarterly*, 63: 22–6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350615.

Markwick, K., Bickerdike, A., Wilson-Evered, E. and Zeleznikow, J. (2019) Technology and family violence in the context of post-separated parenting, *Australian and New Zealand Journal of Family Therapy*, 40(1): 143–62. doi: 10.1002/anzf.1350

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J.P., Shelton, M., Manthorne, C., Churchill, E.F. and Consolvo, S. (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, New York: Association for Computing Machinery (ACM), pp 2189–201. doi: 10.1145/3025453.3025875

Mayhew, J. and Jahankhani, H. (2020) Combating domestic abuse inflicted in smart societies, in H. Jahankhani, S. Kendzierskyj, N. Chelvachandran and J. Ibarra (eds) *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, Advanced Sciences and Technologies for Security Applications*, Cham: Springer International Publishing, pp 347–73. doi: 10.1007/978-3-030-35746-7_16

Messing, J., Bagwell-Gray, M., Brown, M.L., Kappas, A. and Durfee, A. (2020) Intersections of stalking and technology-based abuse: emerging definitions, conceptualization, and measurement, *Journal of Family Violence*, 35(7): 693–704. doi: 10.1007/s10896-019-00114-7.

O'Shea, B., Julian, R., Prichard, J. and Kelty, S. (2019) *Challenges in Policing Cyberstalking: A Critique of the Stalking Risk Profile in the Context of Online Relationships*, in Online Othering, Cham: Springer, pp 331–53. https://link.springer.com/chapter/10.1007/978-3-030-12633-9_14

Parkin, S., Patel, T., Lopez-Neira, I. and Tanczer, L.M. (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, NSPW '19*, San Carlos, Costa Rica: Association for Computing Machinery (ACM), pp 1–15. doi: 10.1145/3368860.3368861

Powell, A. and Henry, N. (2019) Technology-facilitated sexual violence victimization: results from an online survey of Australian adults, *Journal of Interpersonal Violence*, 34(17): 3637–65. doi: 10.1177/0886260516672055

Robinson, A.L., Myhill, A., Wire, J., Roberts, J. and Tilley, N. (2016) *Risk-led Policing of Domestic Abuse and the DASH Risk Model*, London: College of Policing.

Rodríguez-Rodríguez, I., Rodríguez, J.V., Elizondo-Moreno, A., Heras-González, P. and Gentili, M. (2020) Towards a holistic ICT platform for protecting intimate partner violence survivors based on the IoT paradigm, Symmetry 12, 37. doi: 10.3390/sym12010037.

Sambasivan, N., Ahmed, N., Batool, A., Bursztein, E., Churchill, E., Sanely Gaytan-Lugo, L., Mathews, T., Nemar, D., Thomas, K. and Consolvo, S. (2019) Toward Gender-Equitable Privacy and Security in South Asia, *IEEE Security Privacy*, 17(4): 71–7. doi: 10.1109/MSEC.2019.2912727

Slupska, J. and Tanczer, L.M. (2021) Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things, in J. Bailey, A. Flynn and N. Henry (eds) *The Emerald International Handbook of Technology Facilitated Violence and Abuse*, Bingley: Emerald Publishing Limited, pp 663–88. doi: 10.1108/978-1-83982-848-520211049

Slupska, J. (2019) Safe at home: towards a feminist critique of cybersecurity, *St Antony's International Review*, 15: 83–100.

Stark, E. (2007) *Coercive Control: How Men Entrap Women in Personal Life*, New York: Oxford University Press.

Stark, E. (2016) From domestic violence to coercive control in the United Kingdom, *Domestic Violence Report*, 21(2): 23–6.

Stark, E. and Hester, M. (2019) Coercive control: update and review, *Violence Against Women*, 25(1): 81–104. doi: 10.1177/1077801218816191

Sweet, P.L. (2019) The sociology of gaslighting, *American Sociological Review*, 84(5): 851–75. doi: 10.1177/0003122419874843

Tanczer, L.M. (2021) Das internet der dinge: die auswirkungen »smarter« geräte auf häusliche Gewalt, in BFF (Bundesverband Frauenberatungsstellen und Frauennotruf) and N. Prasad (eds) *Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien*, Berlin: transcript, pp 205–25. doi: 10.14361/9783839452813.

Tanczer, L.M. (2019) The government published its draft domestic abuse bill, but risks ignoring the growing threat of tech abuse, Medium, https://medium.com/policy-postings/the-government-published-its-draft-domestic-abuse-bill-but-risks-ignoring-the-growing-threat-of-368a6fb70a14.

Tanczer, L.M., Blythe, J., Yahya, F., Brass, I., Elsden, M., Blackstock, J. and Carr, M. (2018a) *Summary Literature Review of Industry Recommendations and International Developments on IoT Security*, London: Department forDigital, Culture, Media and Sport (DCMS) and PETRAS IoT Hub, https://www.gov.uk/government/publications/summary-literature-review-on-iot-security.

Tanczer, L.M., Brass, I., Elsden, M., Carr, M. and Blackstock, J. (2019a) *The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape, Rewired: Cybersecurity Governance*, Hoboken, New Jersey: Wiley, pp 37–56, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3385548.

Tanczer, L.M., Lopez-Neira, I., Parkin, S., Patel, T. and Danezis, G. (2018b) *Gender and IoT (G-IoT) Research Report: The Rise of the Internet of Things and Implications for Technology-facilitated Abuse*, London: University College London, https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf.

Tanczer, L.M., Patel, T., Parkin, S., Lopez-Neira, I. and Slupska, J. (2019b) *Written Submission to the Online Harms White Paper Consultation*, London: University College London, https://www.ucl.ac.uk/steapp/sites/steapp/files/online_harms_white_paper_consultation_response_giot_june_2019_final.pdf.

UCL STEaPP (2018) UCL runs a digital security training event aimed at domestic abuse support services, *UCL Department of Science, Technology, Engineering and Public Policy*, https://www.ucl.ac.uk/steapp/news/2018/nov/ucl-runs-digital-security-training-event-aimed-domestic-abuse-support-services.

UN Women (2020) Online and ICT-facilitated violence against women and girls during COVID-19, *EVAW COVID-19 Briefs.*, New York: UN Women.

Walby, S. and Towers, J. (2018) Untangling the concept of coercive control: theorizing domestic violent crime, *Criminology & Criminal Justice*, 18(1): 7–28. doi: 10.1177/1748895817743541

Women's Aid (2020) *Our Approach: Change that Lasts*, Bristol: Women's Aid Federation of England.

Woodlock, D. (2017) The abuse of technology in domestic violence and stalking, *Violence Against Women*, 23(5): 584–602. doi: 10.1177/1077801216646277

Yardley, E. (2020) Technology-facilitated domestic abuse in political economy: a new theoretical framework, *Violence Against Women*, 27(10): 1479–98. doi: 10.1177/1077801220947172

Appendix A: Semi-structured interview questions developed and deployed by the Gender and IoT Research Team

Introduction

In your role as XXX, could you explain to us what your **usual engagement** with victims of domestic and sexual violence and abuse looks like?

- What are your **typical timelines** of engagement?

What are services – like the organisation you are working for – **currently doing well** when it comes to the engagement with victims of gender-based sexual and domestic violence and abuse?

- Does **technology play a part** in this?

Tech abuse

How **frequently** do you encounter tech-related abuses when working within the area of victims of domestic and sexual violence and abuse?

Could you elaborate on some of the **most common/most unconventional tech-related risk trajectories, questions, and concerns** you have observed in your work with victims of gender-based sexual and domestic violence and abuse?

What are the **most common technologies** used by perpetrators of domestic and sexual violence and abuse? How do you imagine future IoT devices to be used for abuse?

IoT-facilitated tech abuse

Have you already experienced **IoT devices and services** being of concern when working with victims of domestic and sexual violence and abuse?

- Could you elaborate **which particular IoT risk trajectories** you have encountered?
- Could you describe particular **scenarios**?

In what ways will IoT **impact** your work with victims of domestic and sexual violence and abuse?

- Are there any expected **challenges** that you see arise from IoT?
- Are there any expected **advantages** that you see arise from IoT?

Assessment and documentation

How do you normally **deal with, interact with or provide support** for victims who come to you and have been affected by tech-related abuse?

- Do you draw on particular **guidelines**?
- Do you have a **specific team** helping you?

What **risk assessment/form** are you using when first meeting with a victim of sexual and domestic violence and abuse (for example, SafeLives)?

- What are the **strengths** and **weaknesses** of the risk assessments/forms?
- What **factors** do these documents cover?

Are you **documenting and categorising** tech-related abuse cases during the assessment?

- If not, would the **inclusion** of such a category in the risk assessment/form be **possible** as well as **helpful**?

Support and resources

Have you ever encountered **limitations** where you were not able to help victims of tech abuse?

- **Why** was this the case?
- If not, in what ways do you expect your organisation to **prepare** for such cases in the near future?

To what types of **resources** are you currently referring victims of tech-related abuse?

- **Why** did you choose these resources?
- What are the **strengths** and **weaknesses** of these resources?

To what types of **organisations** are you referring victims of tech-related abuse?

- **Why** did you choose these organisations?
- What are the **strengths** and **weaknesses** of these organisations?

Concerns and design

If you were able ask a specialist any queries you have on your mind concerning emerging technologies such as IoT, what **would you ask**?

- Why?

Imagine you were able to **design the 'perfect device'** that would help victims of domestic violence and abuse. What would the device need to do in order for it to address all of the concerns victims have?

Further research

Do you have any **final questions, points, comments or concerns** you would like to share with the *Gender and IoT* research team?

- What do you hope any **further research** project on the topic to achieve?
- Are there any particular **avenues** for us to further help frontline workers?