Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse

Roxanne Leitão
University of the Arts London
London, United Kingdom
r.leitao@csm.arts.ac.uk

ABSTRACT

This paper presents a design-led qualitative study investigating the (mis)use of digital technologies as tools for stalking, threats, and harassment within the context of intimate partner abuse (IPA). Results from interviews and domestic abuse forum data are reported on and set the foundation for a series of codesign workshops. The workshops invite participants to creatively anticipate smart home attack vectors, based on their lived experiences of IPA. Three workshops with seven IPA survivors and eleven professional support workers are detailed in this paper. Findings are organised into three phases through which survivors' privacy and security needs can be understood: 1) initial purchasing and configuring of smart home devices; 2) daily usage and; 3) (re-)securing devices after abuse has been identified. The speculative attack-vectors and design ideas generated by participants expose, for the first time, survivors' understanding of smart home security and privacy, as well as their needs, concerns, and requirements.

Author Keywords

Intimate partner abuse, Interpersonal privacy, Codesign

CSS CONCEPTS

CCS → Security and privacy → Human and societal aspects of security and privacy → Social aspects of security and privacy

INTRODUCTION

Smart home adoption rates in the UK are currently around 19.7% and expected to reach 39.0% by 2022 [55]. As digital technologies pervade every aspect of our lives, from work to socialising, banking, taxes, shopping, etc., a growing amount of work discusses the misuse of technology to perpetrate abuse [2,16,36,59]. Recent work has also investigated the specific misuse of digital technologies to monitor, stalk, and harass victims of intimate partner abuse (IPA) [18,25,26,31,40,54].

In England and Wales, 27.1% of women, and 13.2% of men experience domestic abuse [44]. It is estimated that around 48% of these cases include technology-facilitated forms of abuse [51]. Although statistics are not yet available for these emerging threats, this year alone, Refuge reported almost 1,000 cases of IPA involving devices such as home hubs and TVs [52].

Existing research into technology-facilitated IPA has mainly taken the form of qualitative interviews or focus groups with survivors and support workers, in the US [20,25,26,40] and Australia [31,60]. Findings focus on current issues, concerns, and barriers that survivors and support workers are facing regarding currently ubiquitous technologies, such as smartphones and social media [18,25,26,31,40,54]. The rapid pace of technological development has meant that cases of IPA involving smart home devices have begun to emerge, whilst victims and support services lack the understanding and resources necessary to cope with these novel challenges. The codesign approach we have taken in this work brings survivors' and support workers' experiences of IPA into the effort of better understanding the challenges that current smart home privacy mechanisms pose to victims of IPA. We hypothesised that issues could be mainly related to shared devices, shared access to remote feeds and usage logs, and different levels of permissions for users in the same household. In this context, both our research questions outlined below, aim to address these two gaps by including survivors and support workers beyond those engaged with support services in the US and Australia and, also, by exploring the challenges posed by smart homes within the context of IPA.

- *Are the current forms of technology-facilitated IPA being faced by survivors in the UK, or engaging in online peer support, the same as those reported by research in the US and Australia?*
- *What are survivors and support workers' main concerns regarding technology-facilitated abuse in the context of near-future smart homes?*

In order to answer these questions, we adopted a codesign methodology alongside IPA survivors. Stage 1 included an analysis of interviews and online forum data to answer the first research question. Stage 2 was informed by Stage 1 and consists of a series of codesign workshops. The codesign process aims to bring survivors and support workers' voices into identifying and speculating on smart home interpersonal privacy issues, based on their lived experience of IPA, which to the best of our knowledge has not been done before.

The results from our interviews and forum data (Stage 1) support previous research, revealing that digital technologies are increasingly being used for monitoring and tracking, remotely threatening and harassing, and non-consensually

DIS '19, June 23–28, 2019, San Diego, CA, USA
© 2019 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-5850-7/19/06…$15.00
https://doi.org/10.1145/3322276.3322366

distributing intimate imagery [20,27,40,60]. They also support the finding that victims and support workers are not equipped to deal with these challenges [25]. An effort to anticipate the ways in which smart homes may exacerbate existing issues led us to Stage 2 of the research. Stage 2 aims to inform the design of smart home privacy mechanisms before they become as widely adopted as smartphones and social media, in an effort to preemptively minimise opportunities for their misuse.

Accordingly, in the Stage 2 workshops, support workers and survivors were guided in using their own experience in imagining possible future smart home attack vectors and envisioning improved future interpersonal privacy scenarios. An attack vector describes the means through which a system and its data may be compromised. In attempting to protect a system, it is essential to understand attack vectors and their context, specifically which assets are being threatened and the potential impact of a breach [43]. In this article, we define speculative attack vectors as those that attempt to predict the vulnerabilities of a system, based on an informed understanding of their usage context. Our speculative attack vectors are grounded in participants' experiences of IPA and aim to predict ways in which future internet-of-things (IoT) devices could be used against victims. Involving users who experience a system under extreme conditions, such as victims of IPA, can contribute to informing the design of smart home privacy and security mechanisms [13,48]. Importantly, not only for this audience but for other non-traditional households (e.g., house shares and multi-family households), in which trust between household members may not be a given.

As expected, an analysis of the codesign workshops shows how survivors and support workers anticipate these issues being exacerbated by the emergence of smart homes. Participants identified attack-vectors that describe the use of IoT devices for the purposes of *gaslighting*, control and intimidation, as well as intimate surveillance. In addition, participants' design ideas provide technologists with insight into their concerns and needs regarding smart home interpersonal privacy.

In summary, this paper contributes in understanding the concerns of survivors and support workers regarding user-privacy in the context of near-future smart homes. It also highlights participants' ideas for improving security and privacy as a means for deterring perpetrators from leveraging such devices for intimate surveillance. Participants' design ideas provide the community with a set of starting points to explore the more inclusive design of smart home privacy and security mechanisms. In addition, our interview and forum data findings extend the reach of existing research on technology-facilitated abuse beyond the US [20,25,26,40] and Australia [31,60], with a UK based study and with an analysis of online forum data that includes stories from survivors, who may not be engaged with professionalised support services.

BACKGROUND AND RELATED WORK

The bodies of work that are useful for contextualising this design-led study of IPA and IoT abuse can be categorised according to 1) technology-enabled IPA, 2) IoT privacy and security, as well as 3) codesign and co-speculation.

This paper firstly outlines related work and then reports on 1) findings from interviews and online domestic abuse forum data (Stage 1) that we considered to be relevant to the Stage 2 investigation on smart homes, followed by 2) findings from the Stage 2 codesign workshops with survivors and support workers. Findings from Stage 2 are separated into participants' speculative smart home attack vectors and participants ideas on how to improve interpersonal smart home privacy mechanisms.

Technology-facilitated IPA

IPA is a global problem and a human-rights issue [15]. Existing research has examined IPA and attempted to characterise different forms of abuse, from physical violence, sexual violence, coercion and control, to emotional and financial abuse [35]. Research investigating the misuse of technology for abusive purposes spans issues such as cyberbullying [29], stalking [34], and online harassment [59]. However, it is important to consider that technology-facilitated abuse within IPA maintains a significant difference from other types of cyber-abuse. In the case of IPA, perpetrators and survivors are not strangers, in fact, they are or have been involved in an intimate relationship. They may be cohabitating, share parental responsibilities, and social networks. This means that perpetrators not only have access to victims and their devices, in the physical world, but may also have intimate knowledge of them, their routines, habits, and preferences.

Particularly relevant to technology-facilitated abuse are the definitions of coercive control and *gaslighting*. The UK Home Office defines coercive control as *"a purposeful pattern of behaviour which takes place over time in order for one individual to exert power, control or coercion over another"* [32]. *Gaslighting* is a form of coercion and control and refers to the process of manipulating someone into doubting their own memory, perception, and sanity. Instances of *gaslighting* can range from denial, by an abuser, that previous abusive incidents took place, up to the staging of unusual events with the intention of disorienting the victim [3].

Within HCI, several authors have begun to investigate the role that digital technologies can play within abusive relationships. Southworth at al. [54] in a 2007 US-based study, found that the same technologies that survivors rely on to access information and support are also the tools enabling perpetrators to monitor, harass, and control their victims. These tools include mobile phones, fax machines, email, GPS, and video recorders. Four years later, Dimond et al. [20] interviewed survivors in a domestic violence shelter, also in the US, about their experiences of technology-facilitated IPA. Participants reported harassment via mobile phones, harassment via social networking sites, as well as the strategies they used to cope based on limited privacy and security knowledge. More recently, Woodlock [60] surveyed survivors and support workers in Australia regarding the abuse of technology in IPA and stalking. The survey found that technology was used to create a sense that perpetrators are omnipresent and inescapable, to isolate, punish, and humiliate victims, as well as to threaten or share non-consensual intimate imagery. The survey also found that perpetrators often have access to victims' phones and either know, can guess, or can obtain login credentials through coercion. Matthews at al. [40] conducted a qualitative study investigating the digital privacy and security needs, challenges, and practices of victims of IPA in New York, US. They propose a framework through which survivors' technology practices and challenges can be understood: *physical control*, *escape*, and *life apart*. In another US-based study, Freed at al. [27] describe a *UI-bound adversary*, in the context of IPA, which consists of an ill-intentioned but authenticated user that interacts with victims' devices/accounts through a standard user-interface, or that downloads software that enables spying on victims. In a separate analysis of the same dataset, Freed at al. [25] find that survivors and support workers are not confident in their ability to deal with technology-facilitated IPA, lacking the necessary expertise, resources, and guidance.

Existing qualitative research on technology-facilitated IPA has focussed on interviews, surveys, or focus groups with survivors accessing professionalised support services in the US [20,25,26,40] and Australia [31,60]. Stage 1 of our work contributes to existing research in two important ways. Firstly, we contribute to the generalisability of existing research by presenting findings from qualitative interviews conducted in the UK. Secondly, we include an analysis of data from three online domestic abuse forums, where victims are engaging in peer-support rather than with professionalised support.

IoT Privacy and Security

The IoT is made up of devices that are internet-connected and able to exchange services and data. Devices range from simple sensors to smartphones and wearables. The IoT enables the creation of smart homes that can include a range of IoT devices, such as smart lightbulbs, door locks, thermostats, security cameras, TVs, etc. The connected nature of the IoT means that users can control devices remotely through a smartphone or computer. A user can, for example, remotely open their front door for a parcel to be delivered, or adjust the house temperature to be warm by the time they arrive.

However, this interconnectedness leads to security blind spots that can leave devices susceptible to breaches and misuse [1,23,33,61]. Researchers have suggested several means for improving IoT security and privacy, from improved device encryption techniques to anonymous data reporting protocols [61]. Nonetheless, although such techniques are helpful, they fail to consider that users are generally the biggest vulnerability in the cybersecurity chain [42,46].

One of the reasons for users being a security vulnerability may, in fact, be related to the usability of security and privacy controls. Poor usability has been shown to lead to inadequate configurations of security settings and/or users finding ways to circumvent security features altogether [42]. Such issues are often exacerbated by users' cognitive state [11], as humans have limited cognitive capacity for information processing and multitasking. As pointed out by West [58], *"[s]ecurity is integrated into systems in such a way that it usually comes with a price paid in time, effort, and convenience—all valuable commodities to users."*. This is especially true for users who may be experiencing high levels of stress and anxiety, which is the case of IPA victims. It is, therefore, unsurprising that research on IPA and technology abuse has found that survivors and support workers often lack the knowledge necessary to effectively manage end-user privacy and security [27,40,60]. Furthermore, smart homes are often *ad hoc* systems, set up by users themselves, without system management resources and without the technical knowledge necessary to effectively manage them [37]. Stage 2 of our research contributes by exposing survivors' and support workers' concerns regarding existing IoT devices' privacy and security, in the form of 1) co-created attack vectors based on participants' lived experience of IPA, and 2) participants' ideas for improving smart home interpersonal privacy.

Codesign & Co-Speculation

Codesign, or participatory design, have been widely used for research and design within sensitive topic areas [6,8,30,38], such as IPA. Codesign is based on the premise that users are experts in their own life circumstances [57] and that everyone is capable of being creative, when equipped with the right tools and environment [50]. It proposes that designers and non-designers collaborate in creating improved and more desirable solutions to the challenges facing participants and their communities. Furthermore, complementary design methods, such as speculative tools, are often used alongside codesign to move beyond immediate need and problem identification, into generative, speculative, and future-oriented ideation [24]. In this work, videos speculating on future IoT products were used to invite participants to engage in conversations and ideation around the near-future of ubiquitous smart homes. Previous work has employed speculative techniques to support codesign participants in futures thinking [17] for the purposes of imagining solutions regarding, for example, the Anthropocene and transformative change [45], getting government officials to collaborate on creating a vision of North Sea sustainability with the aim of influencing global action [30], imagining the future of food [21], and imagining alternative futures for the IoT [19].

This work adopts a codesign methodology, alongside IPA survivors and support workers, in an effort draw upon their experience to inform interpersonal smart home privacy and security design. To the best of our knowledge, survivors and support workers have not been previously involved in using their lived experience to inform design by creatively anticipating IoT attack-vectors that are relevant to IPA.

RESEARCH OVERVIEW

This research took place in the UK alongside several third-sector domestic abuse support organisations. Access to these organisations was established through volunteering and building a relationship between the lead researcher and frontline domestic abuse support workers. Although the researcher is a designer by background, she has received extensive training as part of her volunteering duties and currently supports victims of domestic abuse on a weekly basis. Before beginning the research, ethics approval was sought and received from the university's Research Ethics Committee.

The research design and results are reported according to two stages: Stage 1 refers to the interviews and forum data, while Stage 2 describes the codesign workshops.

STAGE 1: INTERVIEWS AND FORUM DATA

Interview Procedure

Semi-structured interviews were conducted with survivors and professional support workers. Only survivors who were no longer in an abusive relationship were recruited. Interviews explored 1) their experiences of technology being leveraged, by perpetrators, as a tool for abuse; 2) strategies used to cope and defend themselves; 3) gaps in support and information provision; as well as 4) needs for improving existing support. Interviews with survivors were either conducted over video conference calls or at a trained therapist's office. A therapist was present in all interviews with survivors, in case survivors required support during or after the interview. Interviews with professionals took place either remotely or at their work premises. In addition to the questions that we asked survivors, professionals were also asked about their digital security and privacy knowledge, as well as thoughts on and needs for future training. Interviews lasted between 30-95 minutes.

All anonymisation and consent procedures were discussed with interviewees. Participants were also made aware that they could revoke their participation without any negative consequences.

Forum Data Scraping

Web scraping was used to retrieve posts from three domestic abuse forums and then exported in JSON. 200 pages were automatically scraped from each forum, resulting in:

- 189 posts from a specialised DA forum run by an NGO [NGOF], with posts dating between 13.10.17 and 21.11.17;
- 375 posts from a DA community forum [CF], with posts dated between 12.05.12 and 9.07.17;
- 181 from a community DA subforum [CSF], with posts dated between 24.04.17 and 29.07.17.

Forum names have been removed to maintain anonymity. Similarly, any forum transcripts that have been included, to illustrate the findings, are not word for word transcriptions. We have adjusted for abbreviations and language that may be used to identify individuals, corrected grammatical and spelling mistakes, and removed any identifiers (e.g., names, locations), without altering the sentiments, ideas, and/or events being described. This has been done so that a simple search engine query of the transcript will not lead to the original forum post.

Participant Characteristics

Four female domestic abuse survivors [S] were interviewed. Three survivors had children with the former abusive partner and none of them were currently in an abusive relationship. Nine support workers [SW] were interviewed. Seven identify as female and two as male. Professionals came from a variety of third-sector support organisations, including those mainly supporting female victims, professionals supporting victims in same-sex relationships, and others working with perpetrators. Regarding forum data, it is not possible to provide demographics, as most forum users login under a screenname and do not share identifying information.

Interview & Forum Data Analysis

All interviews were transcribed prior to analysis. A thematic analysis was conducted on 754 forum posts and 496 interview excerpts related to accounts of 1) technology being used as a tool for abuse, 2) victims and survivors' use and understanding of technology, as well as 3) support workers' advice on how to deal with technology-facilitated abuse. The excerpts were selected following a thematic analysis, which began by a close reading of the interview transcripts. For the forum data, the initial reading was achieved through a keyword[1] search method followed by a close reading.

An initial phase of descriptive, process, and in vivo coding was carried-out based on the first reading. A codebook was developed, including the name of the code, a description, example transcripts, and connections to other codes. Codes were then iteratively defined and described through a second close reading. A third and final round of axial coding was then performed and followed by a thematic grouping of the codes, which led to the themes detailed below.

INTERVIEW & FORUM DATA FINDINGS

As previously mentioned, the findings below contribute to validating and extending the existing evidence base for technology-facilitated IPA, which in itself is still nascent. They do so by extending the generalisability of previous findings 1) beyond the US and Australia, as well as 2) into survivor communities engaging in peer-support online and who may, or may not, be in contact with support services.

For the purposes of brevity and clarity, we have included only the findings that are most relevant to the codesign workshops. Findings are presented below and each is briefly described and illustrated with a transcript, followed by a reflection on why we believe a particular finding to be relevant to Stage 2's focus on interpersonal privacy and smart homes.

Monitored devices and accounts

Victims discussed the ways through which perpetrators would overtly monitor their devices and online accounts. In these cases, victims are aware that they are under surveillance.

[1] The keywords were: Android; App; Facebook; FB; Computer; Camera; Email; Find my; Find my Phone; Find my Friends; GPS; Hacked; Hacking; Hijack; iMessage; Instagram; Internet; Intimate Photos; Intimate Pics; Intimate Pictures; iPad; iPhone; Keylog; Laptop; LinkedIn; Malware; Monitoring; Pics; Phone; Photos; Porn; Recording; Revenge Porn; Sext; Smartphone; Snapchat; Social Media; Spyware; Stalkerware; Stalking; Tablet; Text; Tracking; Twitter; Video; Webcam; WhatsApp.

> *[CF] He has access to all my emails, my bank account, my phone. Literally everything. Every time I try to get advice from a friend or family member, he goes through my messages. I now have to delete everything.*

In relation to smart home interpersonal privacy: this finding raises questions related to the greater ease of monitoring shared devices that collect data from all household members, as compared to monitoring a victim's personal devices. If personal devices are already being monitored, are there potential risks associated with easy access to, for example, historic usage logs for smart door locks where a perpetrator could potentially monitor the victim's comings and goings?

Hijacked or hacked devices and/or accounts

Victims reported hijacked accounts, where control of an account had either been taken over or an attempt to access it had been made, by the perpetrator. In these cases, either perpetrators had access to victims' login details or attempted unauthorised access to these accounts. However, in some instances, it was unclear how perpetrators were accessing victims' accounts.

> *[S03] Ahm, you know, when the, I'd get a notification that my account had been accessed from a different device, and it would be from, you know, where he was located.*

In relation to smart home interpersonal privacy: hijacking an account may not even be necessary to obtain personal data in the case of shared smart home devices. For example, an Amazon Echo set up with a primary account will accept and log requests from all other users in a household, which will then be available to the owner of the primary account.

Spyware and covert monitoring

Spyware, stalkerware, and covert monitoring were also discussed in the interviews and forums. Spyware is malicious software designed to access and monitor a device and covertly transmit information (e.g., texts, calls, passwords), over a network, to a device of the abusers' choosing. Stalkerware includes spyware but also includes commercial software designed to track children and pets, for example.

> *[S01] And less than 6 months later I found what I thought was something on my phone, brought it to the IT people at my work who were aware of what's going on and they said, "this is how he's been getting", they said, "he knows everything you've been doing". He put, he has a business email and a business STP, or a business server, so he put an ... [hesitation regarding technical terms] SMTP in my phone hidden under one of my email addresses, so everything went through his ...*

The covert nature of spyware, which makes it difficult to identify and remove, made it one of participants' main concerns.

In relation to smart home interpersonal privacy: survivors' experiences of covert monitoring raised a series of concerns, for us, that could be exacerbated by smart homes, such as covert surveillance through remote access to security camera feeds and easy access to device usage logs.

Non-consensual sharing of intimate imagery & Outing

Although not all revenge porn is perpetrated by intimate partners [22], it is nonetheless a concern for participants and was discussed on the forums. For victims in same-sex relationships, the threat of abusers using intimate imagery to 'out' victims to their family and friends was also a concern.

> *[SW03] Most of our [revenge porn] cases, it's part of a much broader pattern of abuse. Quite often there may have been physical abuse, or at least the coercive control type of behaviours is really prevalent. Lots and lots of stalking and harassment, so, and kind of intimidation, so things like impersonating them [victims] on accounts online.*

In relation to smart home interpersonal privacy: the possibility of remotely accessing live indoor home security camera feeds (e.g., Nest Cam) led us to question whether such devices may increase the risk of surveillance and capture of intimate imagery for victims.

Digital privacy & security advice

Often advice, given by professionals or exchanged on the forums, involved changing email accounts, private web browsing, limiting use of the internet and devices, as well as blocking perpetrators' text messages, calls, and emails. Even though participants acknowledged that limiting survivors' participation in the digital sphere can have negative impacts on job prospects, social circles, and other aspects of daily life. Moreover, all interviewed professionals stated that their digital privacy and security knowledge is limited and that, in fact, more training is required.

> *[SW02] It's frightening to think of the effect of the new technology on people where emotion and power is involved and I'm not sure that we know enough to be able to deal with it.*

In relation to smart home interpersonal privacy: the added layers of interpersonal privacy management, associated with smart homes, may pose a significant concern for victims.

The next section reports on Stage 2 of our research. Stage 2 built upon Stage 1's findings on technology-facilitated abuse, to create and run a series of codesign workshops with participants.

STAGE 2: SPECULATIVE WORKSHOPS

Workshops were structured around the following activities:

- Presentation of research findings to date [15 mins]
- Speculative Video 1[2]: Smart Homes [2 mins]
- Group activity: Narrative creation [30 mins]
- Speculative Video 2: Speculative Product Demo [3 mins]
- Group activity: Mapping data misuse [15 mins]
- Group activity: Ideation [30 mins]

The interview and forum data analysis findings, discussed in the previous section, were presented at the beginning of the workshop. The aim was to contextualise the research and inform the group activities.

[2] Workshop materials can be viewed here: [URL removed for anonymity]

Speculative Video 1 illustrated a fully-equipped smart home while contextualising technologies such as indoor cameras and remotely controlled door locks. We refer to videos as speculations due to their intended role in assisting participants in imagining future smart home implications and scenarios in creative ways [7]. The videos set the scene, creating an *imaginarium* upon which participants were then invited to speculate, based on their lived experiences. The video began by framing a utopian vision of the convenience and comfort afforded by smart homes. It then progressively and subtly illustrated scenarios around remote control of household appliances and remote access to feeds of indoor video footage. This was achieved through an aesthetic common to technology promo videos in an effort to highlight technological capabilities in a visual language that users are accustomed to. Most participants were not familiar with smart homes. Therefore, the speculative video, through which an understanding of smart devices and data was built up, was fundamental to the success of the workshops.

Following the first speculative video, participants were asked to create a narrative of how stalking might be perpetrated within the near-future context of a smart home. Each group was either designing for a) a victim cohabitating with the perpetrator, b) a victim living on her own where the perpetrator spends significant amounts of time, and c) a victim who lived with the perpetrator but had recently separated.

A second speculative video was used to set the scene for the data mapping and misuse activity. The video took the form of a short product demo, again following a technology promo aesthetic. The product being presented was framed as a tool that allows users to keep close to their romantic partners, even when both lead busy urban lives. The product claimed to *sync* both parties' phones, allowing users to view each other's location, share their schedules, health and fitness data, as well as follow one another's social interactions. Even though dystopian in nature, the product reflects the capabilities of spyware embedded in a tangible artefact, aiming to aid participants in more fully understanding the abstract capabilities of such covert software. The video contextualises the device and data misuse mapping activity, which sought to encourage participants to consider how smart home devices and data can be exploited by an abusive partner, as well as steps that need to be taken to mitigate misuse.

For the final ideation activity, a series of prompts, in the form of A5 cards, were created to scaffold idea generation. Firstly, participants chose an overarching goal to steer their ideation process. Three goals could be chosen from: 1) "to create opportunities for respite", 2) "to protect victims", and 3) "to empower victims". Secondly, participants selected an issue card, which reflected some of the these identified in Stage 1 (e.g., "monitored devices and accounts") that we found to be relevant to smart homes. Once a goal and an issue had been selected, participants could combine "smart devices" and "interaction/behaviour" cards to support idea generation.

Workshop Participants

Seven survivors [S] of IPA and two support workers [SW] took part in the first workshop, geared towards survivors' experiences. One support worker participated in each group, in case survivors experienced any form of distress. Participants were regular attendees at a local support group and allowed the researcher to run a workshop during one of their meetings. Nine support workers, from two charities, participated in the second and third workshops. The workshops were approved by the organisations' management and participants were given permission to take part during work hours. None of the workshop participants were the same as in the interviews.

Ethics

We are aware that perpetrators may learn from the publishing of these speculative attack vectors. However, recent reports show an increasing trend in the use of IoT devices to perpetrate IPA [18]. We believe that research aimed at speculating on possible future attack vectors will enable technology designers to improve the security and privacy features of near-future consumer devices. Therefore, safeguarding victims by limiting the capabilities of perpetrators to misuse such devices.

Workshop Analysis

Workshops were audio recorded and transcribed for analysis, alongside the written materials completed by participants during the workshops. Following the same approach as described in Stage 1, a thematic analysis was conducted on the workshop transcripts and written materials. In addition to the thematic analysis, a process of sketching and visualising the ideas that participants generated was also employed as a method for analysing content related to design ideation.

Workshop results are reported in two sections. The first details speculative attack vectors and the second describes the design solutions generated by participants.

WORKSHOP FINDINGS: SPECULATIVE ATTACK VECTORS

Three phases were identified that inform the structure we've adopted for reporting participants' speculative attack vectors. The first phase refers to purchasing and/or configuring IoT devices, whether the device is new or is being set up to work with other devices it had not previously been connected to. The second phase includes day-to-day device usage. The third phase describes the (re-)securing of devices/accounts, as well as understanding who has access to which data. This phase occurs when victims need to understand who has access to their data/devices, and in some cases to re-secure their devices/accounts.

Purchasing and configuring smart home devices

When thinking of the ways in which perpetrators may gain access to victims' devices and accounts, participants identified two likely avenues. Firstly, given the nature of IPA, participants described sharing passwords with perpetrators willingly during the "honeymoon" phase [4] of the relationship and before abusive dynamics became apparent, or later being coerced or forced into sharing them.

> *[S01] And who's to say she hadn't given him a password, in the beginning, because she was, she trusted him. Because he used to*

> *stay there, personally you wouldn't let anyone in your house if you didn't trust them. And he was staying there quite frequently.*

Secondly, participants described scenarios in which the perpetrator purchased and configured all household devices. In some cases, this even included victims' personal devices (e.g., fitness trackers).

> *[SW01] So she would've used him [perpetrator], I'm guessing, to set everything up [smart home devices] and relied on him to tell her how they work. And he might've withheld some access permissions from her.*

In doing so, perpetrators could grant themselves access to all devices and data by setting them up to pair with their own accounts. For example, real-cases that were mentioned in the workshop included setting up an Amazon Echo with the perpetrator's Amazon account or gifting the victim with a fitness tracker — essentially a location tracker — that has already been synced with the perpetrator's phone.

> *[SW03] And all the home security device was installed to his phone and not onto her phone so he can see it in every second what she is doing while she has no idea about it.*
> *[SW02] So everything was probably setup on his email, his phone number ...*
> *[SW03] And on, just the application is downloaded to his phone only.*

For us as designers and researchers, regarding the purchasing and configuring of smart homes devices, participants' contributions highlight the following questions: how can devices be designed to automate the creation of multi-user accounts in order to ensure interpersonal privacy? How can users be guided through a setup process that maximises interpersonal privacy?

Daily Usage

During the usage phase, participants mainly identified scenarios related to *gaslighting*, intimidation, control, and surveillance. Professionals and survivors speculated on the misuse of smart home devices, such as locking and unlocking doors, remotely triggering alarms, and changing heating settings, as effective strategies by which *gaslighting* could be perpetrated.

> *[SW01] I supported a client when I first started in [location removed] and they were saying that no one believed them, but her partner was changing the settings of the temperature in the house so that she was really really cold or really really hot. So yeah, I can see quite easily how that would work.*

Many of the same techniques used for *gaslighting* could also be used as tactics to exert control and instil fear. When done covertly, these actions could be seen as attempts to gaslight, whereas when done overtly, they were interpreted as ways for perpetrators to exert power. For example, the granting or revoking smart door lock permissions can be carried out to make victims feel as if they're "losing their mind" or as a form of overtly controlling who is allowed easy access in and out of the house.

> *[SW04] Yeah, I was gonna say, think about tracking the history of all these apps and things, you know. Things like just asking Siri or Alexa or whatever just to "oh, put this music on" and then coming home and [the perpetrator] going "oh, did you enjoy listening to so and so's new album earlier?" That element of knowing what they [the victim] have been doing throughout the day and using that to just remind them that, well, let them know that I [perpetrator] have been watching you [victim]. I know exactly what you've done today.*

In addition to control, participants also discussed the potential of smart devices to be misused for the purposes of overt and/or covert surveillance. Concerns included the use of indoor security cameras to remotely monitor victims inside the house, using smart doorbells to monitor who may visit the victim at home (e.g., a support worker or family member), and using devices, such as baby monitors, that have cameras but that are not immediately obvious as tools of surveillance.

> *[SW01] So, the behaviour, so indoor security cameras, he can spy ...*
>
> *[S01] Mmm. He can see ... he can see ...*
>
> *[S01; S02; S03] ... everything.*
>
> *[S01] Your every move, when you're going and leaving, who got there ... the conversation.*

Finally, regarding daily usage, participants were also concerned with the non-consensual capture of intimate imagery using indoor security cameras, which allow for live feeds to be viewed remotely.

> *[P01] Yeah. And then it opens up a can of worms 'cause if he's watching her, she gets undressed, he could use that against her. Yeah, again just saying "if you don't do this, I'm going to show everyone this".*

Our findings related to daily usage highlight the following design questions: How can permissions between a user in the house and a remote user be better managed to maximise interpersonal privacy? How can access to device usage logs be better managed to maximise interpersonal privacy?

(Re-)Securing devices and accounts

The *blackbox* nature of technology was seen as a problematic factor. Participants were concerned with their own lack of knowledge regarding the data that their own devices collect and with whom this data may be shared. The concern was specifically related to data sharing and unintended leaks between peers, rather than with corporate data misuse. The workshop activities revealed that participants' technical knowledge was incomplete and/or demonstrated a naïve understanding of digital privacy and security. On the one hand, participants tended to overestimate the ease with which IoT devices could be hacked by non-experts.

> *[SW02] So like, Alexa doesn't have a password so there's no technical issues there. The security cameras ... how do you hack into a security camera? You only need to know the IP address ... using an IP address ...*

While on the other hand, they did not seem to have a good understanding of end-user security and privacy settings, nor the knowledge necessary to safeguard themselves.

[S03] Yeah, Facebook does the same thing but it is "near you" or whatever and you can find out whether you're ...

[S02] Can you turn that [Facebook location sharing] off on that?

Understandably, participants were concerned that smart home devices will add significant layers of complexity to managing personal digital privacy and security. They also identified barriers to accessing support from third-parties to deal with the abuse. Participants illustrated scenarios in which victims would attempt to seek support by reporting the technology-facilitated abuse to the police or discuss it with a trusted contact, only to be told that the devices may be malfunctioning or that the victim does not know how to use them correctly. In fact, professionals also demonstrated concern over the "believability" of such cases, wondering whether they themselves would find accounts of smart homes being used for abuse credible.

[SW04] Or if it's the technology. How quick are we to blame technology for stuff not working?

[SW02] "Oh, there's a fault in there" or "the systems not working".

[SW01] Well, you can hear it right now, can't you? You can just hear the person saying "Oh, you know ..."

[SW04] "... it glitches".

Even if believed, professionals' gaps in knowledge regarding technology-facilitated abuse may leave victims at risk. On the one hand, victims could be given advice that makes their situation worse. On the other hand, a lack of confidence in professionals' capabilities in this area may mean that victims won't attempt to access the required support.

[P03] Problem is when you do go to the police, they don't actually work on the area [technology-facilitated abuse] that you're needing to discuss and they don't understand it."

Even though victims may wish to re-secure their devices/accounts and regain access control, a lack of knowledge in this area and an absence of confidence in support services may stop them from being able to do so. Even if achieved, participants were concerned that attempts to regain control may lead to an escalation in abuse.

[SW03] The main problem with all this is if you snooze it [smart home hub] then the perpetrator will know what you are doing so you are scared to snooze it. Instead, you are letting all the devices run in the background. 'Cause if you weren't scared to snooze it then you wouldn't be scared to leave the [house] ...

[SW01] ... but you could find your opportunity, couldn't you? So, you could wait until they'd left the room or something. Or ...

[SW02] ... but wouldn't it show on the log, like "snoozed at 5:45 pm"?

Finally, regarding (re-)securing devices and accounts, we highlight the following questions*: How can users be guided through a setup process that maximises interpersonal privacy? Should all adults in a household be automatically granted the same level of permissions? How can device controls be designed to facilitate managing interpersonal privacy on shared devices?*

WORKSHOP FINDINGS: IDEATION

In addition to identifying attack vectors, participants also co-created ideas for improving the interpersonal privacy of smart home devices. This section details participants' ideas.

Privacy and Security Information and Visualisations

All participants expressed uncertainty as to where and how data is stored. As previously mentioned, technology, especially the cloud, was seen as a *blackbox* system that is impenetrable to users. Several of the ideas generated during the workshop involved visualising where data is being stored as well as who has access to it. Participants expressed the desire for an "awareness" app which would display, in one place, all the personal data gathered by all devices. The app would also visualise who has access to an individual's personal data, alongside any data sharing changes that may have been affected by system and app updates.

[SW01] I think what would be good would be some kind of ahm ... So, exactly what [data sharing] is switched on and what is switched off, that gives you a map, a map of apps and devices. So, you know exactly what's going on with your devices.

Robust multi-user support

Although smart home hubs allow for the creation of multiple user accounts, this requires a somewhat cumbersome process that places the burden on users, as well as requiring a non-trivial degree of technology-related knowledge [6,28]. During the workshops, participants discussed issues surrounding the use of shared accounts and easy access to another user's account within the same household. The former could occur if the perpetrator configured a home hub to use a single account and did not then grant the victim permission to create another one. The latter can occur if users forget to switch between accounts before using the hub.

In this context, automatic creation of accounts, based on the recognition of different users' voices was suggested. In other words, instead of the system relying on users to configure an account for each household member, the system would automatically detect different voices and assign them an account each. Users would then only have access to the account and data associated with their own voice.

[SW01] Making it not one device fits all. Then making it that like you have to identify who you are before you use it so then it goes to your personal [account] not one [shared] account.

Multi-Factor Authentication and biometrics

Linked to the previous design idea was participants' interest in multi-factor authentication. In the context of IPA, perpetrators often have access to victims' devices and knowledge of their login credentials. Especially in the case of covert surveillance, fingerprint or voice authentication could prove effective in hindering perpetrators' access to victims' devices.

[SW02] Yeah, so if I was going to access the picture on my phone and I was going to send it in an email, a fingerprint then

would validate that it's me sending the picture [concern over non-consensual access and sharing of intimate pictures].

Furthermore, as previously mentioned, participants were concerned with the use of indoor security cameras for surveillance and/or the capturing of non-consensual intimate imagery. In this context, participants suggested that such devices should require an additional level of authentication from users who are in the house. For example, if a user is trying to access a live video feed while another user is at home, the system should require an additional level of authorisation from the user in the home.

[SW01] But is then permission [to access remote camera feeds] maybe is [sent to] like a mobile number or something that is completely separate so that the person gets it and then ...

[SW04] Yeah.

[SW01] You know and independently can say [yes or no] ...

Improved visual and auditory affordances

Devices recording and storing data in the background were extensively addressed in the ideation activity. Participants' design ideas largely focussed on improving user-awareness of when data is being recorded, especially video and audio. In order to achieve this goal, participants proposed improved visual and auditory affordances. For example, indoor security cameras emitting a sound every hour when they're recording, or smart home hubs making it more obvious when they're on and listening through larger visual or auditory cues.

[SW01] But then if you had a [indoor security] camera that like every hour had to beep, then you'd know if something was there.

Usability of privacy and security controls

Participants expressed difficulty in managing digital privacy and security, especially when under stress. Participants argued for improving the transparency and usability of such controls, as well as digital privacy and security for the general public.

[SW02] What for me, what I think is, it's very easy to use technology, so you don't have to be an IT expert to access this stuff and use it but in order to protect yourself you need to be an expert.

[P05] You need to be a bloody genius.

Spyware removal

Participants expressed difficulty in detecting spyware and a general concern over the means through which spyware could be installed in the first place. Participants equally feared that spyware would progress beyond smartphones and move onto devices such as smart home hubs, TVs, etc. In order to address this issue, built-in spyware detection software was proposed.

[SW01] And that would be the same for all of them [smart home devices], wouldn't it? So, I wonder if, you know you get spyware now [for these devices]?

[SW03] And some sort of like anti-spyware for it?

[SW06] Just "Alexa, run spyware scan".

DISCUSSION

The interviews and forum data, from Stage 1, provided insight into our first research question: *are the current issues being faced by survivors in the UK or engaging in online peer support, regarding technology-facilitated abuse, the same as those reported by existing studies in the US and Australia?*

Our findings show that survivors and support workers in the UK, and victims seeking peer support online, are facing the same challenges as those highlighted by research conducted in the US [20,25,26,40] and Australia [31,60]. Issues include monitoring communications and social media, location tracking, hijacked accounts, digital harassment and abuse, and the capture of non-consensual imagery [18,25,26,31,40,54]. This knowledge enabled us to more confidently design the workshops and build on existing knowledge, in order to sensitively and appropriately explore the topic of technology-facilitated IPA and near-future smart homes with participants. We felt it would be inappropriate, and potentially insensitive, to begin addressing this near-future challenge if participants' current experience did not already involve forms of technology-facilitated abuse. The aim of focussing on the near-future was to inform the design of IoT devices before they become as widespread as the technologies already being leveraged for abuse — smartphones and social media.

These findings led us to the second research question: *what are survivors and support workers' main concerns regarding technology-facilitated abuse in the context of near-future smart homes?*

Overall, our research found that participants were concerned about the privacy and security complexities added by 1) the shared nature of smart home devices and accounts, 2) the possibility of viewing historic usage logs that include data for all household members, and 3) being able to remotely access live video feeds of the home. Participants felt that these "features" could enable direct surveillance — in the case of security cameras and live video feeds — or forms of more indirect surveillance through monitoring usage logs, such as smart door lock logs, household members' shopping activity, or even queries made to smart home hubs (e.g., Amazon Echo).

Importantly, underlying these concerns is the fact that participants already felt overwhelmed with the current challenges of managing their privacy and security regarding smartphones and social media, expressing the opinion that smart homes would significantly exacerbate these already unmanageable challenges. Participants did not believe they had the knowledge and competencies necessary to manage their own digital privacy and security, which in the case of IPA may have serious consequences. Unsurprisingly, participants felt that the best way to protect themselves was to opt-out of using such devices altogether.

This work, operating within the context of IPA, shows that the design community needs to broaden the scope of user needs and requirements considered in the development of smart home devices. It is essential that users operating within non-traditional "idealised" households and cohabitation structures be included in the process. Much of the research on smart home privacy has focussed on privacy from corporate or third-party data collection [8,14,47]. Our interest lies in interpersonal privacy between users sharing a household [19], particularly when the relationship between users is abusive in nature and the data is, therefore, susceptible to being exploited for nefarious purposes.

It is in this context that this research points to the need for considering privacy between individuals when designing devices for shared usage. Participants' ideas, for improving smart home interpersonal privacy, also highlight a fundamental tension between an absolute necessity for IPA survivors to safeguard their privacy and a gap in knowledge that would enable them to do so effectively. This aligns with previous research on the usability of privacy and security controls [5,38,39]. It means not only that privacy notifications and settings need to be as clear and easy-to-use as possible, but also that systems should be designed with privacy in mind in order to remove some of the burden of protecting their own privacy from users.

Drawing on examples from the codesign workshops, we highlight the need for multi-user devices that are easier to setup with multiple accounts, where the default privacy settings protect individual household member's data from each other. For example, a smart thermostat may turn on the heating when one of the users is in the house, which would reveal, in aggregated historic logs when a member of the household was in or out of the home. This raises a series of questions, such as: *how can devices be designed to automate the creation of multi-user accounts in order to ensure interpersonal privacy? How can access to device usage logs be better managed to maximise interpersonal privacy?*

There is also a need to rethink permissions between users located in the home and those accessing a system remotely. For example, a few questions arise when a user is attempting to access a live feed of an indoor security camera, while another is in the house — *How can users be guided through a setup process that maximises interpersonal privacy? How can permissions between a user in the house and a remote user be better managed to maximise interpersonal privacy?* The questions raised by our research with IPA survivors and support workers point to directions for further investigation in the design of privacy mechanisms for shared home devices. We ask *how* and not *if* because such privacy mechanisms are technically possible to implement but research has yet to assess the most effective ways of realising them in a manner that is inclusive, accessible, useful, and usable.

The consequences of devices designed around a lack of understanding regarding different users' context can be more harmful than designers originally imagine. This work illustrates the experiences of a group who may be seriously impacted by such devices, resulting in situations that may place them at more risk of abuse, harassment, and violence.

Limitations

Our sample is not representative of all IPA survivors and support workers. Instead, our aim was to understand a small subset of stories' and contributions in detail through a qualitative design-led research methodology. The codesign workshops, scaffolded by the speculative IoT videos, were effective in encouraging participants to imagine near-future scenarios and predict the potential challenges posed by smart homes for IPA victims and survivors.

CONCLUSION

Over 8 million adults in the UK suffer from IPA and recent reports suggest that technology-facilitated abuse, through IoT and smart home devices is on the rise [10,53]. However, given the relatively low IoT device adoption rates [55,56], existing research on technology-facilitated IPA has mainly focussed on abuse enabled by smartphones and social media [25,26,31,40,54]. It has also largely been conducted in the US [20,25,26,40] and Australia [31,60] with professional support workers and survivors accessing professionalised services.

Our work contributes to existing research by including an analysis of 1) data from interviews conducted in the UK, and 2) data from survivors accessing peer-to-peer support online, who may not be involved with professional services. In this manner, our findings support and add reliability to the findings documented in previous work, by extending the geographic reach and extending the audience beyond those engaging with professional support.

Furthermore, the findings from the codesign workshops, which engage survivors and support workers in creatively anticipating near-future smart home attack vectors and imagining better futures, are a novel contribution to the privacy design community. Firstly, participants' speculative attack vectors draw upon their experience of IPA and have been organised into three phases: 1) purchasing and configuring smart home devices, 2) daily usage, and 3) (re-)securing devices and accounts, through which survivors' experiences can be understood. Secondly, participants ideas for improved privacy and security, more than necessarily constituting viable designs, provide insight into their needs, requirements, and understanding of digital privacy. This work allows the wider design and technology communities unprecedented insight into IPA victims' smart home privacy and security understanding, concerns, needs, and requirements.

ACKNOWLEDGEMENTS

We would like to thank all the participants for their time, courage, and willingness to contribute to research.

REFERENCES

[1] Mohamed Abomhara and Geir M. Køien. 2014. Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 1–8.

[2] Elias Aboujaoude, Matthew W. Savage, Vladan Starcevic, and Wael O. Salame. 2015. Cyberbullying: Review of an Old Problem Gone Viral. *Journal of Adolescent Health* 57, 1 (July 2015), 10–18. DOI:https://doi.org/10.1016/j.jadohealth.2015.04.011

[3] Kate Abramson. 2014. Turning up the Lights on Gaslighting. *Philosophical Perspectives* 28, 1 (December 2014), 1–30. DOI:https://doi.org/10.1111/phpe.12046

[4] Parveen Azam Ali and Paul B. Naylor. 2013. Intimate partner violence: A narrative review of the feminist, social and ecological explanations for its causation. *Aggression and Violent Behavior* 18, 6 (November 2013), 611–619. DOI:https://doi.org/10.1016/j.avb.2013.07.009

[5] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 787–796. DOI:https://doi.org/10.1145/2702123.2702210

[6] Amazon. 2018. Help: Household Profiles on Alexa Devices. *Amazon: Help & Customer Service*. Retrieved September 21, 2018 from https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201628040

[7] Andrew Darby, Anna Whicher, Emmanuel Tsekleves, and Naomi Turner. 2015. *ProtoPolicy: Using Design Fiction to Negotiate Political Questions*. Lancaster University. Retrieved from http://eprints.lancs.ac.uk/78341/1/ProtoPolicy_Design_Report_Print.pdf

[8] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *arXiv:1708.05044 [cs]* (August 2017). Retrieved April 5, 2019 from http://arxiv.org/abs/1708.05044

[9] Erling Björgvinsson, Pelle Ehn, and Per-Anders Hillgren. 2012. Agonistic participatory design: working with marginalised social movements. *CoDesign* 8, 2–3 (June 2012), 127–144. DOI:https://doi.org/10.1080/15710882.2012.672577

[10] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *The New York Times*. Retrieved January 5, 2019 from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[11] Michael W. Boyce, Katherine Muse Duma, Lawrence J. Hettinger, Thomas B. Malone, Darren P. Wilson, and Janae Lockett-Reynolds. 2011. Human Performance in Cybersecurity: A Research Agenda. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 55, 1 (September 2011), 1115–1119. DOI:https://doi.org/10.1177/1071181311551233

[12] Deana Brown, Victoria Ayo, and Rebecca E. Grinter. 2014. Reflection Through Design: Immigrant Women's Self-reflection on Managing Health and Wellness. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 1605–1614. DOI:https://doi.org/10.1145/2556288.2557119

[13] Jed R. Brubaker and Janet Vertesi. 2010. Death and the social network. In *Proc. CHI Workshop on Death and the Digital*.

[14] J. Bugeja, A. Jacobsson, and P. Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, 172–175. DOI:https://doi.org/10.1109/EISIC.2016.044

[15] Charlotte Bunch. 2018. Transforming Human Rights from a Feminist Perspective. *Women's Rights, Human Rights*. DOI:https://doi.org/10.4324/9781315656571-2

[16] Sloane Burke Winkelman, Jody Oomen-Early, Ashley Walker, Lawrence Chu, and Alice Yick-Flanagan. 2015. Exploring Cyber Harassment among Women Who Use Social Media. *Universal Journal of Public Health* (September 2015), 194–201. DOI:https://doi.org/10.13189/ujph.2015.030504

[17] Stuart Candy and Jake Dunagan. 2017. Designing an experiential scenario: The People Who Vanished. *Futures* 86, (February 2017), 136–153. DOI:https://doi.org/10.1016/j.futures.2016.05.006

[18] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, 441–458. DOI:https://doi.org/10.1109/SP.2018.00061

[19] Audrey Desjardins, Jeremy E. Viny, Cayla Key, and Nouela Johnston. 2019. Alternative Avenues for IoT: Designing with Non-Stereotypical Homes. In *CHI Conference on Human Factors in Computing Systems Proceedings*. DOI:https://doi.org/10.1145/3290605.3300581

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

[21] Marketa Dolejsova. 2018. Edible Speculations in the Parlour of Food Futures. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI EA '18), alt13:1–alt13:10. DOI:https://doi.org/10.1145/3170427.3188406

[22] EIGE. 2017. *Cyber violence against women and girls*. European Institute for Gender Equality. Retrieved from

http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls

[23] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security analysis of emerging smart home applications. In *Security and Privacy (SP), 2016 IEEE Symposium on*, 636–654.

[24] Laura Forlano and Anijo Mathew. 2014. From Design Fiction to Design Friction: Speculative and Participatory Design of Values-Embedded Urban Technology. *Journal of Urban Technology* 21, (December 2014), 7–24. DOI:https://doi.org/10.1080/10630732.2014.971525

[25] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* 1, CSCW (December 2017), 46:1–46:22. DOI:https://doi.org/10.1145/3134681

[26] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), 667:1–667:13. DOI:https://doi.org/10.1145/3173574.3174241

[27] Diana Freed, Jackeline Palmer, DMΨKLΦ Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. (2018).

[28] Google. 2018. Set up multiple users for your speaker. *Google Home Help*. Retrieved September 21, 2018 from https://support.google.com/googlehome/answer/7323910?hl=en

[29] Dorothy Wunmi Grigg. 2010. Cyber-Aggression: Definition and Concept of Cyberbullying. *Journal of Psychologists and Counsellors in Schools* 20, 2 (December 2010), 143–156. DOI:https://doi.org/10.1375/ajgc.20.2.143

[30] Maarten A. Hajer and Peter Pelzer. 2018. 2050—An Energetic Odyssey: Understanding 'Techniques of Futuring' in the transition towards renewable energy. *Energy Research & Social Science* 44, (October 2018), 222–231. DOI:https://doi.org/10.1016/j.erss.2018.01.013

[31] Bridget A. Harris and Delanie Woodlock. 2018. Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies. *Br J Criminol* (2018). DOI:https://doi.org/10.1093/bjc/azy052

[32] Home Office. 2015. Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/482528/Controlling_or_coercive_behaviour_-_statutory_guidance.pdf

[33] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling Multi-user Controls in Smart Home Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (IoTS&P '17), 49–54. DOI:https://doi.org/10.1145/3139937.3139941

[34] Jordana N. Navarro. 2016. Cyberabuse and Cyberstalking. In *The Intersection Between Intimate Partner Abuse, Technology, and Cybercrime*. Carolina Academic Press, Durham, North Carolina, 125–140.

[35] Joan B. Kelly and Michael P. Johnson. 2008. Differentiation among types of intimate partner violence: Research update and implications for interventions. *Family court review* 46, 3 (2008), 476–499.

[36] Robin M. Kowalski, Gary W. Giumetti, Amber N. Schroeder, and Micah R. Lattanner. 2014. Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological bulletin* 140, 4 (2014), 1073.

[37] Huichen Lin, Neil Bergmann, Huichen Lin, and Neil W. Bergmann. 2016. IoT Privacy and Security Challenges for Smart Home Environments. *Information* 7, 3 (July 2016), 44. DOI:https://doi.org/10.3390/info7030044

[38] Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (IMC '11), 61–70. DOI:https://doi.org/10.1145/2068816.2068823

[39] M. Madejski, M. Johnson, and S. M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 340–345. DOI:https://doi.org/10.1109/PerComW.2012.6197507

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

[41] J. McIntyre-Mills. 2010. Participatory Design for Democracy and Wellbeing: Narrowing the Gap Between Service Outcomes and Perceived Needs. *Syst Pract Action Res* 23, 1 (February 2010), 21–45. DOI:https://doi.org/10.1007/s11213-009-9145-9

[42] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts. 2011. Guidelines for usable cybersecurity: Past and present. In *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, 21–26. DOI:https://doi.org/10.1109/CSS.2011.6058566

[43] J. R. C. Nurse, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese. 2015. Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In *2015 International Workshop on Secure Internet of Things (SIoT)*, 5–14. DOI:https://doi.org/10.1109/SIOT.2015.10

[44] ONS. 2016. Intimate personal violence and partner abuse. *Office for National Statistics*. Retrieved February 15, 2017 from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/compendium/focusonviolentcrimeandsexualoffences/yearendingmarch2015/chapter4intimatepersonalviolenceandpartnerabuse

[45] Laura Pereira, Tanja Hichert, Maike Hamann, Rika Preiser, and Reinette Biggs. 2018. Using futures methods to create transformative spaces: visions of a good Anthropocene in southern Africa. *Ecology and Society* 23, 1 (2018), 19.

[46] Shari Lawrence Pfleeger, M. Angela Sasse, and Adrian Furnham. 2014. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management* 11, 4 (2014), 489–510. DOI:https://doi.org/10.1515/jhsem-2014-0035

[47] Miloslava Plachkinova, Au Vo, and Ala Alluhaidan. 2016. Emerging Trends in Smart Home Security, Privacy, and Digital Forensics. *AMCIS 2016 Proceedings* (August 2016). Retrieved from https://aisel.aisnet.org/amcis2016/ITProj/Presentations/23

[48] Graham Pullin and Alan Newell. 2007. Focussing on Extra-Ordinary Users. In *Universal Acess in Human Computer Interaction. Coping with Diversity* (Lecture Notes in Computer Science), 253–262. DOI:https://doi.org/10.1007/978-3-540-73279-2_29

[49] Nithya Sambasivan, Julie Weber, and Edward Cutrell. 2011. Designing a phone broadcasting system for urban sex workers in India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 267–276.

[50] Elizabeth B.-N. Sanders and Pieter Jan Stappers. 2008. Co-creation and the new landscapes of design. *Co-design* 4, 1 (2008), 5–18.

[51] Snook, Chayn, and SafeLives. 2017. *Tech vs Abuse: Research Findings*. Comic Relief. Retrieved from http://media.wix.com/ugd/f86f13_366b6514c8fc4e9488fc15edf2148d52.pdf

[52] Sonia Elks. 2018. Domestic abusers using internet, smart devices to spy on and control partners, women's group says. *The Globe and Mail*. Retrieved September 14, 2018 from https://www.theglobeandmail.com/world/article-domestic-abusers-using-internet-smart-devices-to-spy-on-and-control/

[53] Sonia Elks. 2018. Smart devices - a new tool for domestic abuse. *Reuters*. Retrieved January 5, 2019 from https://uk.reuters.com/article/britain-tech-women-idUKL8N1VK53G

[54] Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. Intimate Partner Violence, Technology, and Stalking. *Violence Against Women* 13, 8 (August 2007), 842–856. DOI:https://doi.org/10.1177/1077801207302045

[55] Statista. 2018. Smart Home - United Kingdom. *Statista Market Forecast*. Retrieved September 14, 2018 from https://www.statista.com/outlook/279/156/smart-home/united-kingdom

[56] Statista. 2018. Smart Home - United States. *Statista Market Forecast*. Retrieved September 14, 2018 from https://www.statista.com/outlook/279/109/smart-home/united-states

[57] Toni Robertson and Jesper Simonsen. 2012. Participatory Design: An Introduction. In *Routledge International Handbook of Participatory Design*. Routledge, London, 1–18.

[58] Ryan West. 2008. The Psychology of Security. *Commun. ACM* 51, 4 (April 2008), 34–40. DOI:https://doi.org/10.1145/1330311.1330320

[59] Janis Wolak, Kimberly J. Mitchell, and David Finkelhor. 2007. Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts. *Journal of Adolescent Health* 41, 6, Supplement (December 2007), S51–S58. DOI: https://doi.org/10.1016/j.jadohealth.2007.08.019

[60] Delanie Woodlock. 2016. The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women* 23, 5 (May 2016), 584–602. DOI: https://doi.org/10.1177/1077801216646277

[61] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. 2017. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal* 4, 5 (October 2017), 1250–1258. DOI: https://doi.org/10.1109/JIOT.2017.2694844