TECHNOLOGY-FACILITATED INTIMATE PARTNER ABUSE:

ADDRESSING THE ISSUE THROUGH CODESIGN WITH SURVIVORS AND SUPPORT WORKERS

A Thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of the Arts London.

Roxanne Leitão
Central Saint Martins
February 2021

Supervisory team
Dr. Matt Malpass, Central Saint Martins
Prof. Lorraine Gamman, Central Saint Martins
Dr. Peter Hall, Central Saint Martins

ABSTRACT

This PhD work aimed to better understand how 1) existing and near-future digital technologies are used as tools for abuse and surveillance within the context of intimate partner abuse (IPA), and 2) to design support solutions for survivors.

In order to do so, a codesign methodology was adopted alongside IPA survivors and NGO support workers.

The first phase of the work aimed to extend existing knowledge of the landscape and problem context through interviews with survivors and support workers, as well as an analysis of online forum data where survivors engage in peer-to-peer support. The results allowed for a better understanding of the different ways in which technology-

-facilitated abuse is perpetrated, how victims make use of technology within the bounds of an abusive relationship, as well as the gaps in professional and peer advice given to victims regarding digital privacy and security.

The second phase consisted of several codesign workshops with survivors and support workers, which focussed on smart home devices and IPA. In the workshops, we collaboratively understood the threats posed by novel smart-home devices, how these devices are used for surveillance and abuse, the support currently available to victims, and, as before, survivors' and support workers' gaps in digital privacy and security knowledge. We also codesigned a series of ideas for improving the support available to victims regarding digital privacy and security management, alongside a series of ideas for improving the interpersonal privacy afforded by smart home devices.

The final stage involved developing a support service — in this case, a chatbot — to address the issue of technology-facilitated IPA alongside participants, as well as a co-evaluation of the outcome. The codesigned chatbot is now entirely owned and maintained by one of the largest UK-based charities supporting victims of IPA.

ACKNOWLEDGEMENTS

There are so many people who have supported me in many different ways during my PhD. First and most importantly, I want to thank all the people who participated in the research and talked to me so openly about their experiences. Due to confidentiality, their names must remain anonymous. I am also indebted to all the NGOs that agreed to participate in the research, for their enthusiasm and for always making me feel welcome despite the inevitable disruption such a partnership entails.

I would also like to thank my supervisors Dr Matt Malpass, Prof Lorraine Gamman, and Dr Peter Hall for their insightful comments, encouragement, and for the hard questions that challenged me at several key moments of my research.

An enormous thank you to my family and friends who have been extremely supportive of my research and the long hours committed to it. Mitchell Leitão, Caroline Claisse, Amelia Knowlson, Dani Davies, Ana Angel, Bahbak Hashemi-Nezhad, Yemima Safra, Christina Skarpari, Jen Poage, Tobias Yu-Kiener, and Ray Kinsella, thank you for all the chats, coffees, discussions, guidance, and also the fun we've had throughout the process.

Finally, this research would not have been possible without the PhD scholarship and support received from the London Doctoral Design Centre, the Design Against Crime Research Centre, and University of the Arts London.

ABBREVIATIONS

Children and Family Court Advisory and Support Service (CAFCASS)

Crime Survey for England and Wales (CSEW)

Domestic abuse (DA)

Domestic Violence Intervention Project (DVIP)

Female-genital mutilation (FGM)

Human-computer interaction (HCI)

Instant messaging (IM)

Internet-of-things (IoT)

Intimate partner abuse (IPA)

Minimal viable product (MVP)

Office of National Statistics (ONS)

Operating System (OS)

Participatory design (PD)

Research Ethics Committee (REC)

Social internet-of-things (SIoT)

United Kingdom (UK)

United States (US)

User-interface (UI)

Victim Support (VS)

Violence Against Women and Girls (VAWG)

DEFINITIONS

Gaslighting refers to behaviours intended to make another person doubt their own sanity, memory, and sense of reality. Such behaviours include denying facts and events that took place, purposeful misinformation and contradiction. For example, denial by an abuser that previous abusive incidents occurred is a common form of *gaslighting.*

Interpersonal privacy refers to the disclosure, or not, of information about an individual to others with whom they have an interpersonal relationship. Interpersonal relationships can be, but are not limited to, familial, romantic, or friendly relationships.

Stalkerware is software that enables an individual to monitor another individual's device, such as a smartphone, remotely. It can be installed on the device with or without the owner's permission and can be overt or covert in its tracking and monitoring activities.

Technology-facilitated abuse includes all behaviours that involve the use of technology as a means to coerce, stalk, monitor, or harass another person.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1

INTRODUCTION

1.1 RESEARCH MOTIVATION

The motivation for this research can be placed within the context of the global economic crisis of 2008, the European austerity agenda, and the resulting budget cuts to domestic abuse (DA) support services in the UK (Buchan, 2017; Conley, 2012; Jones, 2014). Within the context of my practice as a designer-researcher in the field of Human-Computer Interaction, this work began with an interest in how digital technologies could be leveraged to improve third-sector DA support services (see Fig. 1) despite increasing resource constraints. Through initial desk-based research and then volunteering work with a DA support charity, I came to realise that a range of novel threats had also emerged with the proliferation of digital consumer technologies — they were being misappropriated by perpetrators to further control, harass, and intimidate victims. Manifestations of this behaviour included tracking victims' locations, hijacking and/or monitoring their devices and accounts, as well as threatening to release intimate photographs. Third-sector support organisations, who were already under a great deal of strain, were not prepared, nor did they have the in-house knowledge, to support victims on issues of digital privacy and security. These novel threats, posed by technology, led to a reframing of my research to focus specifically on technology-facilitated abuse within the context of intimate partner abuse (IPA). Technology-facilitated intimate partner abuse refers to perpetrators' use of digital technologies for stalking, monitoring and surveillance within the context of a romantic relationship (Woodlock, 2016).

The ways in which women[1] are subject to a disproportionate amount of abuse, threats, and intimidation online have been well documented. Including high-profile cases, such as Anita Sarkeesian, who has been the target of over 5 years of ongoing online abuse and death threats for criticising the portrayal of women in video games (Webber, 2017), and Sue Perkins, whose life was threatened on Twitter, due to rumours that she may replace a male colleague on a popular TV show (Baird, 2015).

A recent UK study on the prevalence and impact of online trolling of members of parliament (MPs) revealed that the impact of online trolling was far greater on female MPs than on male MPs (Akhtar and Morrison, 2019). Akhtar and Morrison (ibid.) surveyed 181 MPs focussing on online social media abuse and its effects. They found that female MPs were subject to a wider variety of forms of abuse, with the majority of abuse being personal in nature (e.g., racial and sexual abuse). Abuse targeted at male MPs, on the other hand, was largely confined to their professional duties and abuse on political grounds. The study also highlighted that female MPs suffered more emotional stress and damage to their reputation as a consequence of online abuse.

Almost a quarter (23%) of women, surveyed across eight countries, said they had experienced online abuse or harassment at least once (Amnesty International, 2017). Although these particular forms of cyber-aggression are being perpetrated by strangers, who do not know their victims, they are a reflection of the hegemonic power structures within which technology development, cyber-aggression, and DA are embedded.

The well-documented lack of diversity in digital technology development and design (Evans and Rangarajan, 2017; Harrison, 2019; Rangarajan and Evans, 2017; Wachter-Boettcher, 2017) alongside the widespread belief that technology is neutral of values and politics (Noble and Roberts, 2019) has led to an industry of White male supremacy that fails to take into account the perspectives of women and people of colour (Goulden, 2019; Noble and Roberts, 2019). Similarly, funding cuts to DA services, alongside the fact that most victims are women (Office for National Statistics, 2016), and the amount of time it has taken for abusive behaviours between intimate partners to be criminalised (Matczak, Hatzidimitriadou and Lindsay, 2011), can be interpreted in light of imbalances of power resulting from a lack of diversity in policy and law making (Conley, 2012) where women and minorities are underrepresented as compared to national demographic data. Technology development has long been a process lacking in workforce diversity and therefore believed to reflect the values and needs of an unrepresentative

1 When the word "woman" is used in this dissertation, it refers to all those who identify as women. This PhD draws on evidence about gendered violence from secondary sources that, as far as I can ascertain, rarely mention whether both cisgender and transgender women have or not been included. This matter may need further research investigation but is beyond the scope of this PhD.

sample of the population (Evans and Rangarajan, 2017). Recent research investigated 4 digital assistants' responses to health-related queries, namely Apple's Siri, Google Now, Samsung's S Voice, and Microsoft Cortana. What they found is that although assistants responded effectively to queries regarding heart attacks or suicidal thoughts, they were unable to respond to queries related to sexual assault or DA, both of which disproportionately affect women (Miner *et al.,* 2016).

Furthermore, and of particular relevance to this work, is the finding that almost half of the DA victims surveyed by Snook *et al.* (2017) reported that abusers were using digital consumer technologies to further harass, control, intimidate, and threaten them. More recently, *Refuge*, the UK's largest DA charity, says that 72% of its service users experience abuse through technology (Refuge, 2020). In light of these findings, *how do we prevent technology being used as a tool for abuse? And how can we reframe and rethink the design of digital privacy and security to include a more diverse set of users?*

Since the 1970s there have been arguments calling for design to move away from the constraints imposed by its formalisation, as a discipline, in mass-manufacturing, towards socially-engaged design practices. From Papanek (1972) to more contemporary authors (DiSalvo *et al.,* 2011; Thorpe and Gamman, 2011; Björgvinsson, Ehn and Hillgren, 2012; Manzini and Coad, 2015) there is a proposition that social design refers to "the concepts and activities enacted within participatory approaches to researching, generating and realising new ways to make change happen towards collective and social ends, rather than predominantly commercial objectives" (Armstrong et al., 2014, p. 15). It is in this context that this work attempts to approach, the issue of technology-facilitated IPA, from a social and collaborative design perspective.

1.2 RESEARCH QUESTIONS

In order to frame the inquiry, structure the practice, as well as set the project's aims and objectives the research questions presented below were created.

Can codesign with victims of technology-enabled domestic abuse (DA):

> *… make a difference to understanding where the system of getting help and support breaks down?* [RQ1]
>
> *… help enable the production of viable innovative design solutions to address this national (and global) challenge? [RQ2]*

… inform how design studies understand codesign as a process of generative inquiry in addressing complex social problems? [RQ3]

Fig. 1. DA support services

1.3 AIMS & OBJECTIVES

In line with the underlying motivation for the research — enabling victims and support workers to take back control of cyber-privacy and -security issues — and with the research questions, these are the aims of this work:

1. Contribute to the theoretical understanding of codesign methods for working alongside vulnerable participants.
2. Contribute to knowledge on the ethics of codesign with vulnerable participants.
3. Assess whether design can develop effective IoT-based support solutions for DA victims of cyberstalking and abuse.

In order to achieve these aims, measurable and identifiable objectives that will allow for tracking progress, have been identified:

- Collect victims' experiences of seeking support and identify gaps in current services.

- Develop codesign methods appropriate for sensitive contexts where both victims and non-victims are participating.
- Contribute to discourse on the roles of the designer-researcher as a designer and facilitator within codesign.
- Codesign and develop prototype solutions alongside victims and support workers.
- Evaluate the prototypes within real-world settings.

1.4 RESEARCH METHODOLOGY

As previously stated, this work involved DA support workers and survivors in codesigning solutions to different forms of technology-facilitated abuse within intimate relationships. Visions of design being used as one of many tools to address complex social issues has a long tradition (Dantec and DiSalvo, 2013; DiSalvo, 2012; Manzini and Coad, 2015; Papanek, 1972). Social design places emphasis on designers' responsibility to address real human needs and contribute to human wellbeing rather than manufacturing false desires through the design of products for mass consumption (Thorpe and Gamman, 2011; Bardzell, 2018). Social design often employs codesign methods to work alongside communities in creating shared understanding, knowledge, and *solutions* to shared issues of concern (Manzini and Coad, 2015, pp. 48–49). This practice stands in political opposition to top-down approaches common in other research and design methods where the researcher/designer studies and intervenes on the community without collaborating with the community itself (Robertson and Simonsen, 2012). Within this PhD, the aim was to work collaboratively with IPA survivors and support workers to understand the problem context and co-create solutions to address the issue of technology-facilitated IPA. Therefore, a codesign methodology was adopted.

The codesign practice broadly followed the Design Council's Double Diamond process for design and innovation projects (Ball, 2019). Although I acknowledge the process is not as linear as depicted in Fig. 2 and the Design Council has continuously evolved the Double Diamond process for the same reason (Drew, 2019), I believe it is still a useful framework to provide a simplified overview of this PhD's codesign work. Accordingly, in the *Discover* phase, to understand where existing support structures were failing, firstly, an analysis of data from online DA discussion forums was performed. Followed by semi-structured interviews with support workers and survivors. An analysis and synthesis of the findings allowed for defining the problem space of technology-facilitated IPA — Define — and formed the basis of the codesign workshops.

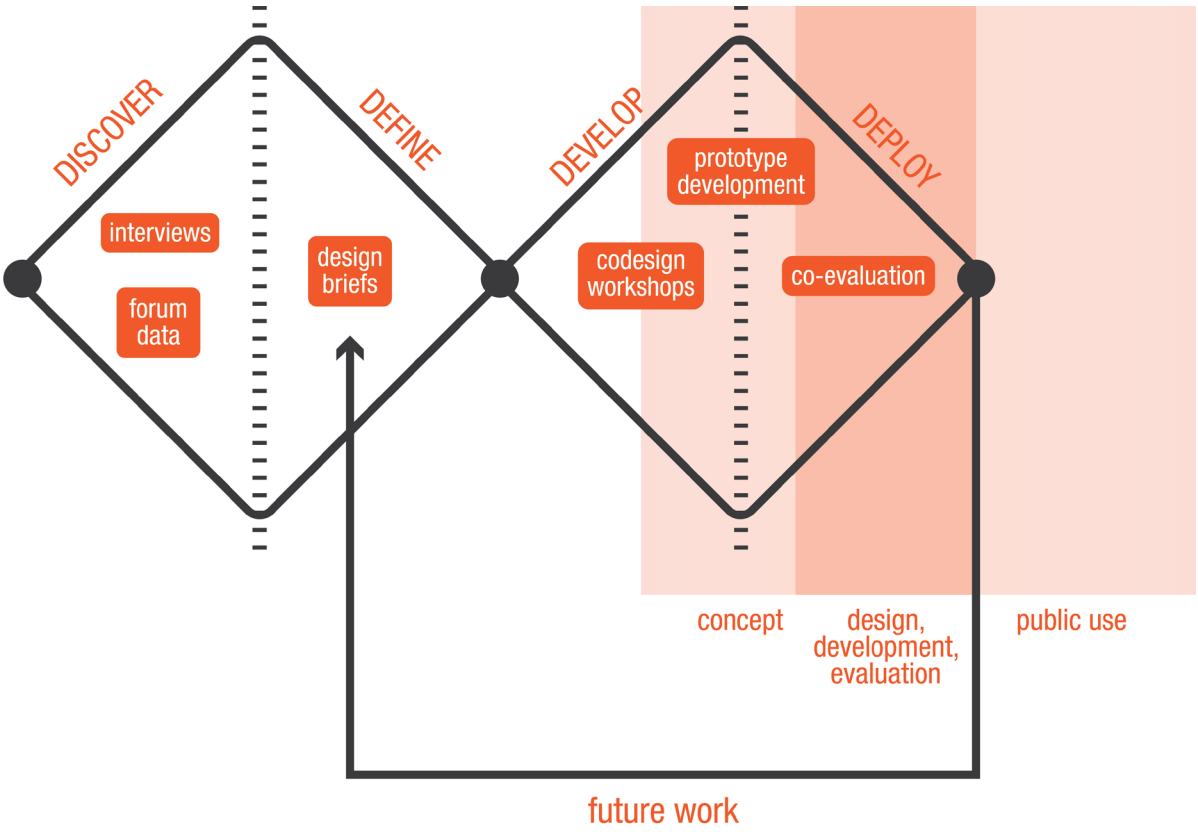

Fig. 2. Methodology

In the *Develop* stage, survivors and support workers were involved in a series of codesign workshops (Bratteteig *et al.,* 2012) looking at the threats and design opportunities posed by current, or near-future, consumer smart home technologies. A thematic analysis (Saldana, 2015) approach was adopted for analysis of the interviews, forum data, and codesign workshops and is reported on in Chapters 3 and 4 respectively.

One of the co-developed ideas was selected and developed into a functional chatbot. In the *Deploy* phase, a co-evaluation of the prototype was conducted alongside participants, and then implemented live on *Refuge's* website. A process of handing over ownership of the chatbot ran alongside design and development, in order to ensure that the NGO was ready to host and maintain the output once this PhD work reached an end. At this point in time, *Refuge* has full ownership of the chatbot, videos, and all its content.

In parallel, efforts to create the socio-technical infrastructures needed to realise a codesign project (Björgvinsson, Ehn and Hillgren, 2010; Dantec and DiSalvo, 2013) took place throughout the duration of this PhD, as described in the next section.

1.5 *INFRASTRUCTURING* THE CODESIGN PRACTICE

Infrastructuring has been proposed as a term to describe the continuous work of creating and aligning shared interests between all parties involved in codesign, as well as managing the conflicts and social relationships between individuals (Björgvinsson, Ehn and Hillgren, 2010; Dantec and DiSalvo, 2013). It also includes building trust with codesign partners, which is especially relevant to codesign within sensitive topics areas such as DA. The process of *infrastructuring* this PhD work began through a series of volunteering activities with three NGOs across London, specialised in supporting victims of DA. Those organisations were Respect, Victim Support (VS), and the Domestic Violence Intervention Project (DVIP).

I received training from each of the organisations and was involved in directly supporting victims with both VS and DVIP for over 2 years, on a weekly basis. Support was delivered either over the phone (DVIP) or face-to-face at an outreach centre (VS). My volunteering duties with Respect were slightly different as I helped them to create a new website, which brought together the different support services they offered to male victims of DA.

The volunteering took place throughout the first 36 months of the PhD and started around 12 months before any participant recruitment for the research took place. During the volunteering and once the research activities had begun, my relationship with these organisations evolved into one of mutual trust. Trust allowed them to assist me in recruiting their own staff and IPA survivors to take part in the codesign. They also introduced me to other NGOs/charities in the field, such as *Refuge,* and, as a consequence, different organisations were involved in different phases of the research.

Without this process of *infrastructuring*, initially through volunteering and through the research activities themselves, I do not believe it would have been possible for me, as an outsider, to involve survivors in a process of codesign that was safe and aware of everyone's needs. The training and the good will of NGO staff, in reviewing my research materials, was essential for this work to adapt and become appropriately sensitive to the context in which it was operating.

1.6 FORMAT AND ROLE OF PRACTICE

Codesign argues for the participation of non-experts in the design of the processes, products, and infrastructures that will form a part of their daily experiences (Simonsen and Robertson, 2012, p. 2). This work involved survivors of DA and support workers in the design process, from problem framing, to ideation, prototyping, refining, and evaluating. Thus, creating and designing mechanisms for participant involvement was one of the main roles that the practice embodied. In addition, and given my background in UX design, the practice also involved developing an interactive chatbot and the refinement of codesigned concepts into a functional prototype.

Outputs of my practice, as a UX designer, can be found at roxanneleitao.com/practice/ and include:

- a website and video to support NGOs in recruiting survivors and explaining the research;
- materials designed to promote collaborative problem context-setting and ideation within the context of technology-facilitated IPA;
- videos designed to communicate abstract concepts such as smart homes and stalkerware;
- an instance of the chatbot, which is now live at refuge.org.uk.

1.7 THESIS STRUCTURE

This subsection explains the structure of the thesis and introduces its main contents. The chapters in this document follow the order in which the practice took place and should be read in sequence.

Chapter 1 provides an introduction to the dissertation, alongside research questions, aims and objectives, research methodology, as well as the format and role of practice.

Chapter 2 serves to position the research within existing discourse and practice. In particular, it addresses DA, technology-facilitated IPA, and participatory design. This review has informed the selection of participants for the codesign activities, as well as informed the structure and analysis of the interviews and online forum data, reported on in Chapter 3.

Chapter 3 includes an analysis of data gathered from interviews with DA support workers, survivors, as well as data from online discussion forums. This analysis has revealed the main technology-facilitated IPA affecting DA victims and survivors, as well as the gaps in support services relating to issues of digital security and privacy. It informs the design briefs that structure the codesign workshops of Chapter 4.

Chapter 4 describes the codesign workshops with survivors and support workers. It includes a description of the procedures and materials used in the workshops, followed by the findings from the workshops. The findings are organised into five themes that cover the use of smart home technology to perpetrate abuse (Themes 1-2), victims' strategies for coping (Theme 3), gaps in current support provision for victims (Theme 4), and participants' codesigned ideas for addressing technology facilitated-IPA (Theme 5).

Chapter 5 outlines the development of one of the codesigned ideas alongside a DA charity. It details the technical implementation of a chatbot and development of all its content.

In Chapter 6, the process of co-evaluating the chatbot is described. This chapter includes the procedure followed in the co-evaluation sessions and their consequent analysis. It then reports on the findings of the co-evaluation and the design modification that were made to the chatbot as a result.

Chapters 3 to 6 all include elements of the practice of codesign, from interviews to workshop design, data analysis, co-ideation, and co-evaluation of outputs. Each of these chapters concludes with a discussion of the findings and, where relevant, of the codesign process itself.

The thesis closes with Chapter 7, which answers the research questions, describes the contribution to knowledge, and sets out future work.

1.8 SUMMARY OF CONTRIBUTION

The recent increase in technology-facilitated abuse within the context of IPA (Refuge, 2020) means that research and design have not yet reached an in-depth understanding of the issue and ways to address it. Studies have emerged over the past decade in Australia and the US (Dimond, Fiesler and Bruckman, 2011; Woodlock, 2016; Freed *et al.*, 2017; Matthews *et al.*, 2017; Harris and Woodlock, 2018) whilst studies in the UK on technology-facilitated IPA have been less frequent (van Moorsel et al., 2011; Snook

et al., 2017). The rapid pace of technological change requires such studies to be more frequent in order to keep pace with the adoption of novel consumer technologies. For example, recent media stories point to the use of smart home technologies for the purposes of abuse (Bowles, 2018; Elks, 2018) yet there is a lack of research investigating this novel problem.

Furthermore, research and design involving survivors and support workers in understanding the problem context and ideating solutions collaboratively has, to the best of my knowledge, not been attempted before. Existing research focusses on understanding and describing the problem context and dynamics of technology-facilitated IPA (Dimond, Fiesler and Bruckman, 2011; Woodlock, 2016; Freed *et al.,* 2017; Matthews *et al.,* 2017; Harris and Woodlock, 2018). Therefore, in this context, this PhD work contributes in the following ways:

- It extends existing knowledge on technology-facilitated IPA, how it is perpetrated, the gaps in existing support provision, and problematizes the need for survivors to be experts in digital privacy management to protect themselves. It does so by building upon existing work conducted in the US and Australia, with perspectives from UK-based NGOs and survivors seeking online peer support.
- It is a first successful attempt to include survivors and support workers in co-creating a tool that tackles the issue of technology-facilitated IPA by providing visual instructional information on digital privacy. A tool that is now owned and updated by an NGO belonging to the community.
- This work has also been a first attempt at involving survivors of abuse in anticipating digital privacy threats, which in this case were related to smart homes.

2

CONTEXTUAL REVIEW

There are currently more objects connected to the internet than there are people in the world (Statista, 2018a). Connected consumer devices range from fitness trackers, thermostats, door locks, fridges, smart TVs, to jewellery, and smartphones (Fig. 3). The relatively small group of corporations responsible for the majority of these consumer devices, such as Google, Samsung, Apple, and Amazon, is notorious for issues related to the lack of workforce diversity, where women and minorities are underrepresented as compared to national demographic data (Evans and Rangarajan, 2017). This reinforces existing hegemonic structures of power, where the historically underrepresented continue to not influence how the connected world develops.

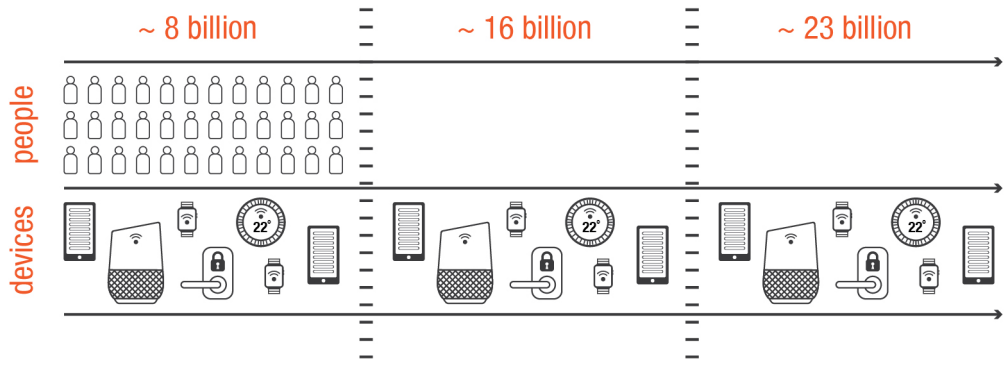

Fig. 3. Amount of devices and people in 2018 (Statista, 2018a)

This chapter discusses socially engaged codesign that aims to bring the voice of a marginalised group of citizens — victims of intimate partner abuse — into the processes of designing the smart home products and services that are, or will be, part of their daily lives. It then presents an overview of the problems posed by novel technologies within the context of intimate partner abuse (IPA). The aim of this chapter is to contextualise codesign as the methodology chosen to address the issue of technology-facilitated abuse within intimate relationships, with a focus on near-future smart homes.

2.1 SOCIALLY-ENGAGED CODESIGN

Socially engaged design aims to address *matters of concern*[1] that are not already being engaged with by the markets or the state. In order to contextualise socially-engaged codesign, I begin with an introduction to the types of problems that design is thought to be well suited to address. This is followed by a deeper look into socially engaged codesign practices and the *infrastructuring* of such projects. Finally, the ethical considerations of involving "vulnerable" participants in codesign are discussed.

2.1.1 INTRODUCTION

Wicked problems are problems that are difficult or impossible to solve due to incomplete, contradictory and ever-changing networks of requirements (Rittel and Webber, 1973). They are subject to ongoing redefinition and the efficacy of any proposed ***solutions*** is, thus, near impossible to evaluate. In fact, the evaluation of solutions takes place through their implementation in real-life contexts, and therefore, cannot be easily undone whether successful or not (Coyne, 2005). Examples are the implementation of public programmes to address ***wicked problems*** such as homelessness, poverty, and urban renewal. Rittel and Webber (1973, p. 60) propose the concept of ***wicked problems*** in a rejection of the notion that all problems can be understood through a positivistic approach, or in other words, through the application of the scientific method alone. They argue that the problems addressed by the natural sciences, and in many cases by the engineering professions, are *"definable and separable and may have solutions that are findable"* — they are *tame problems* rather than the *wicked problems* that are societal issues.

This definition of *wicked problems* was not alone in opposing a positivistic interpretation of the world. A reaction against the design science approaches of the 1960s and their focus on understanding, documenting, and describing design methods can also be observed during this time (Michel, 2007, p. 42). Schön (1983) describes the process of designing as a "conversation with the materials of a situation" (Schon, 1991, p. 78), that is not susceptible to being summarised and captured into a set of discrete steps or methods. He argues that designers enter into a reflective process with the situation they are attempting to address, by producing *things* and then adapting to the intended and unintended consequences that those things have on the situation — designers

1 Latour (2008) describes *matters of concern* as the consequence of gatherings of ideas, forces, players and circumstances in which things and issues, not facts (or *matters of fact*), come to be and to persist, because they are supported, cared for, worried over.

reflect-in-action as their understanding of the problem changes, along with their strategies for action, and models of the issue. Their process is, therefore, appropriate for addressing dynamic problems that are not fully mapped-out — *wicked problems.* Moreover, this process is often tacit and subconscious, making it very difficult for designers to articulate it, in a systematic manner, that can be captured into succinct methods or steps to be followed.

Similarly, Cross (1982) proposes that design is particularly well suited to address *wicked problems*. Cross (ibid.) observes that design activity is generally more concerned with generating solutions, rather than on a deep and prolonged analysis of a problem. If the problem is a *wicked problem*, then, in fact, it may never be fully understood before attempts to tackle it are made. Therefore, *wicked problems* are less susceptible to exhaustive analyses and may be better addressed by the solution-focussed approach of design. Three decades later, focussing on socially engaged design, Thorpe and Gamman (2011) argue for socially responsive design, in which all the actors involved in a codesign process are required to be responsive to the dynamic nature of the *wicked problems* being addressed, whilst acknowledging the constraints that are imposed upon them by existing political and social structures of power. Thorpe and Gamman (2011) place socially responsive design within the context of participatory design, which I will now consider in more depth.

2.2 PARTICIPATORY DESIGN (PD) & CODESIGN

This contextual review will continue with a brief discussion of the historical context of codesign and its origins in participatory design (PD), followed by a contemporary overview of codesign practice applied to social issues. Before doing so, it would be relevant to note that much of the evolution towards participatory modes of design overlaps in time with the previously discussed opposition to the scientific method when presented as the only way to interpret the world and address problems.

In 1972, Victor Papanek wrote, in the context of the social and political responsibilities of design, *"[i]n an age of mass production when everything must be planned and designed, design has become the most powerful tool with which man shapes his tools and environments (and by extension, society and himself). This demands high social and moral responsibility from the designer. It also demands greater understanding of*

the people by those who practice design and more insight into the design process by the public" (p. ix).

Similarly, in an anthology of papers called "Design for Need, The Social Contribution of Design", following a 1971 symposium at the Royal College of Art in London, Dickson (1977) discussed the role that technology plays in mediating human interaction with the material world. He argued that in doing so, technologies transmit a particular set of "material meanings" that represent and convey ways of dealing with the material world, that in turn influence the ideologies and politics of any given period in time. The example of the parallel rise of factory systems of production and industrial capitalism is given to illustrate this point. For a contemporary example, one can look at the invention of the internet, the commodification of knowledge, and the rise of what has been termed "technocapitalism" (Suarez-Villa, 2012). Dickson (1977) concludes by saying that for any new technology to succeed it must match society's priorities, and if those priorities need to be changed to create a more equal and fair society, then technologies need to be developed collaboratively alongside individuals and efforts for change. In the same anthology, Nuttall (1972) posits that designers need to join "the people" in an effort to collaboratively build urban environments that support and promote the unique needs, dreams, and desires of each and every individual. He puts forward the idea of the designer as a technical advisor who provides "a vast and subtle range of methods" to engage a multitude of actors and non-experts in design.

In a similar manner and during the same decade, Scandinavian Participatory design (PD) emerges. Codesign is said to have its origins in the Scandinavian tradition of PD and the Workplace Democracy Movement of the 1970s, which mainly focused on novel systems design alongside employees in factory settings. It emerged as a reaction to automation and the introduction of computers into the workplace, with the aim of providing better tools to support people in their tasks, while enabling them to keep their jobs, learn new skills, and relegate the repetitive less-skilled assignments to machines (Simonsen and Robertson, 2012, p. 2). Schuler and Namioka (1993, p. viii) propose that PD was mainly concerned with enabling a more *"humane, creative, and effective"* relationship between technology designers and the people who use the technologies, which would subsequently lead to a better match between technological systems and human activities. In much the same way, codesign is understood as the collaborative creative process between designers and non-designers working together in the design development process (Sanders and Stappers, 2008). PD is built on the understanding that individuals are experts in their own life circumstances, and that

when adequately supported by a design team, can become designers themselves (Robertson and Simonsen, 2012).

More than 40 years after the emergence of PD, Manzini (2015) ties the (re)emerging field of social innovation and codesign together in his book *"Design, When Everybody Designs: An Introduction to Design for Social Innovation".* Social innovations can be defined as novel products, services, or infrastructure that addresses social needs and create new social collaborations. They are good for society while also enabling society to take action. Manzini (Ibid.) argues that in the contemporary context of rapid and constant technological and social transformation, everybody is a designer in that we all design our own identities and life projects in an effort to improve our current state of affairs, effectively viewing individuals as experts in constructing their own life experiences. However, and even though he argues that design is a widespread human capability, the author proposes that for it to be of use it must be adequately understood and cultivated. Manzini (ibid.) distinguishes between *diffuse design* (performed by everybody) and *expert design* (performed by those who have been trained as designers) and describes how they interact. He maps what design experts can do to trigger and support meaningful social changes, focusing on emerging forms of collaboration. Much in the same way as in Nuttall (1972), professional designers are seen as those who have developed the specific knowledge needed to allow them to operate professionally in the design process. Within the context of socially engaged codesign, their responsibility is seen as being twofold. On the one hand, the designer's role is to aid in the sensemaking, or understanding, of complex social issues so that they may be addressed by all the actors in a codesign process (DiSalvo *et al.,* 2011). Designers have long been understood to be particularly effective in drawing connections, mapping-out complexity, and deconstructing chaos — or in other words, sensemaking (Kolko, 2009). On the other hand, the designer's role can be seen as one of visualising, communicating, and prototyping envisioned solutions within the codesign process (Sanders and Stappers, 2008).

The tradition of involving non-experts in design for social innovation has gained a great deal of traction over the past decade (Ehn et al., 2014). It has been used as a methodology to address a wide-variety of social issues, of which I will only mention a few that are more directly related to this work. Examples are projects aimed at 1) improving the safety of sex-workers in India; 2) working with minority groups of female immigrants and refugees towards economic empowerment and integration into Swedish society; 3) identifying health challenges and designing solutions with immigrant women from the

Caribbean where domestic abuse (DA) was one of the main themes proposed by the participants; as well as 4) designing policy and public services alongside participants from Aboriginal communities in Australia, again where one of the themes of focus was DA (McIntyre-Mills, 2010; Sambasivan, Weber and Cutrell, 2011; Björgvinsson, Ehn and Hillgren, 2012, p. 136; Brown, Ayo and Grinter, 2014).

Social design aims to tackle problems that are not commonly addressed by the markets nor by the state, and in which the affected people do not normally have a voice — generally because they do not possess the economic and political capital to be permitted a voice (Ehn et al., 2014; Manzini and Coad, 2015). Codesign can be seen as a means of involving otherwise invisible communities and of making *matters of concern* public (DiSalvo *et al.,* 2011). Additionally, by working alongside participants and communities in building and intervening in the world, socially engaged codesign can create new forms of knowledge that are inaccessible through other methods such as interviews and ethnography. It engages participants in using their tacit knowledge, and life experience, in critically engaging in a collaborative process of ideation and design. It then allows for the intervention/solution to be experienced, evaluated and reflected upon by all those involved. This allows participants to assess the efficacy of solutions but also to reflect on the new challenges and the shifts that the solutions may provoke.

This work approaches IPA as a *wicked problem* that is a human rights issue and a political matter, which influenced the choice of methodology. IPA is political, as defined by (Mouffe, 2005), in the sense that it sits within configurations of power relations, and hegemonic structures, and cannot be understood outside of the dimensions of agonism that emerge in these relations (Weissman, 2007). It is in this context that socially engaged codesign has been proposed as a methodology to work alongside IPA support workers and survivors, in addressing the novel challenges posed by everyday technologies being used as tools for abuse. Accordingly, the following subsection contextualises existing work on *Infrastructuring* socially engaged codesign projects.

2.2.1 *PUBLICS, MATTERS OF CONCERN,* AND *INFRASTRUCTURING* A SOCIALLY ENGAGED PROJECT

Codesign has become increasingly interested in the notion of public and *publics* (Dantec and DiSalvo, 2013), which are defined by Dewey (1927, p. 15): *"[t]he public consists of all those who are affected by the indirect consequences of transactions to such an extent that is it deemed necessary to have those consequences systematically cared for".*

Given that the public is not a constant entity but rather a product of its environment and conditions, Dewey argues that *publics* are multiple and mutable in that they are formed around significant issues of concern that are themselves subject to ongoing change, which brings me back to previously mentioned *wicked problems.*

Latour (2004) refers to the gathering of support, care, and worry, or the emergence of *publics* in Dewey's terminology, around certain matters as what transforms them into collective *matters of concern. Matters of concern* do not depend on being agreed upon as facts but rather constitute issues, facts, events, which are of collective concern. Latour (ibid.) gives the example of weapons of mass destruction and the American war in Iraq as an example of something that emerged as a *matter of concern* large enough to mobilise entire nations but was not necessarily a *matter of fact.* Use of the word *concern* indicates that collective care for a particular issue, matter, or movement need to be in place whether or not it is a *fact.* In a similar way to how Dewey sees *publics* forming around significant issues of concern that depend on context, environment, conditions that are mutable in time. Bellacasa (2011) builds upon *matters of concern* with feminist concerns for care. For Bellacasa, the aim of representing *matters of concern* as *matters of care* is to expose invisible labours of care in *matters of concern* and also to generate care. Generating care is meant as the actions of paying attention to participants and issues who have not been successful, or are unlikely to succeed, in articulating their concerns, or whose politics are marginalised by opposition to prevalent ways of understanding. She calls for asking questions such as *whose interests are represented, and whose labours are erased? Who or what is or is not counted or assembled here and why?* (Bellacasa, 2011, p. 93). Bellacasa argues that thinking of *matters of fact* as *matters of care* can be a commitment to speculating on how things may be different if they generated care, where care is re-examined in accordance with context to address questions such as *Who cares? What for? Why do we/they care? How do we/they care?*

Papacharissi (2015, pp. 8–9) proposes that through the sharing of affect online, internet technologies, such as social media, may facilitate the formation of networked publics, from previously disorganised crowds, around shared issues of concern. The increasing importance of the digital realm means that not only are people living more of their lives online, but that many of the issues of concern that existed before the internet, are now being observed online (e.g., cyber-bullying, -stalking, and -harassment). *Matters of concern* moving from the physical to the digital, and the overlap between them, are relevant to this work as it investigates technology-facilitated forms of IPA. Furthermore, this work is concerned with drawing attention and worry for those who can be harmed

by an assemblage but whose voices are less valued, as are their concerns and need for care (Bellacasa, 2011, p. 92) — victims of technology-facilitated IPA who are being harmed through digital technologies and smart home devices, for which they are neither responsible nor have the power to change.

The process of constituting and supporting *publics* around physical and/or digital *matters of concern*, from the point-of-view of codesign interventions, has been termed *infrastructuring.* It describes the continuous work of creating and aligning shared interests between all parties gathered around an issue of concern, as well as managing the conflicts and social relationships between individuals. It is not seen as limited to the design project, but includes the sociotechnical infrastructures that were already in place before a project, and those that will go on after a design intervention is cocreated and adopted into use (Björgvinsson, Ehn and Hillgren, 2010). Rice (2017) refers to the human (socio) and nonhuman (technical) actors and infrastructure, involved in codesign, as an ongoing evolving network. This work aims to contribute, through the use of codesign, to the formation of a public around the issue of concern that is technology-facilitated abuse between intimate partners.

Finally, as designers and researchers pursue the goals of socially-engaged design, and strive to *infrastructure* projects alongside communities, or *publics,* affected by a common *matter of concern*, a series of ethical considerations are raised. Especially if the communities that are affected by a particular issue are perceived to be "vulnerable". The following section discusses the ethics of codesign within sensitive contexts more thoroughly.

2.2.2 THE ETHICS OF CODESIGN WITHIN SENSITIVE CONTEXTS

As part of the process of ethical review of this work, issues such as participant anonymity, confidentiality, and autonomy were raised. I will focus on a review of these components within the context of codesign and research with "vulnerable" participants.

As previously discussed, codesign implies shared ownership over the design process and outcomes, where all parties are involved in codesign and cocreation, and therefore, have equal share in the project's successes and failures. Thus, denying participants the ability to receive adequate recognition for the work can be seen as directly opposing their autonomy and right to be credited. Within this project, questions such as *"Do*

participants want to keep ownership of their life stories? Do participants want to lend their identity to their own stories?", and *"Do participants want to be credited, in full, for their participation in the research?"* began to surface. However, it seems the current process of ethics review, and the guidelines for ethical research that are in place, do not allow researchers to ask such questions, nor discuss confidentiality preferences with potential participants, especially if the participants are considered to be "vulnerable"— which is in itself a fuzzy concept (Levine *et al.,* 2004).

Commonplace approaches to participant confidentiality and anonymity come from a tradition of biomedical research, and large sample sizes, where it is possible to aggregate anonymised data without losing context and meaning. Anonymisation is widely accepted as a means of protecting participants from mental health- and social-related risks, by allowing participants to freely express their experiences and opinions without fear of stigmatisation or retribution. However, some authors argue that in qualitative research, with its reduced sample sizes, anonymity may, in fact, be near impossible to achieve (Hoonaard, 2003). Especially when research is being conducted within community settings, as codesign often is, or when snowball sampling techniques are used. Although ethical guidelines have evolved and been adapted to sociological research, design research, and participatory research, the default adoption of participant anonymity has largely gone unchanged, even if it has been challenged (Boman and Jevne, 2000; Ryen, 2004; Giordano *et al.,* 2007; Svalastog and Eriksson, 2010).

Downes at al., (2014) argue that the often excessive scrutiny to which Research Ethics Committees subject research involving marginalised groups, leads to less research and, therefore, a dangerous lack of understanding, as well as an insufficient evidence-base for different types of interventions. This, in turn, contributes to the further marginalisation of such groups who continue to be underrepresented in funding, research, as well as consequent state and social interventions. Downes at al. (ibid.) also argue that given the fact that 1 in 4 women will have experienced domestic and/or sexual abuse in their lifetime, most social research has the potential to involve victims/survivors of abuse. What is more, if victims/survivors are classified as belonging to a "vulnerable" group, and therefore having limited capacity to make their own decisions, alongside children, the long-term ill, the bereaved or the institutionalised, this effectively categorises the majority of the population as "vulnerable" (Downes, Kelly and Westmarland, 2014, p. 3). Mulla and Hlavka (2011) argue that in categorising victims of violence as "vulnerable", we run the risk of assuming they have diminished or impaired capacity to give consent. This would imply that, as legal subjects, their ability to consent to a domestic violence

case being taken to court is compromised, or in cases of sexual violence, their ability to consent to medical treatment and forensic procedures could also be challenged.

Participatory research with victims of DA, such as that reported by (Clarke *et al.,* 2013) and (Bhuyan *et al.,* 2005) reveals that often anonymity and confidentiality with different participants needs to be negotiated, as not all participants wish to be anonymised to the same extent. This demonstrates that a one-size fits all approach is not always appropriate for participatory research projects. It also aligns with the principles of confidentiality set out in The Belmont Report, which argue that "To show lack of respect for an autonomous agent is to repudiate that person's considered judgments" (The National Commission for the Protection of Human Subjects, 1979, p. 4) cited in (Newman and Kaloupek, 2009).

Assuming that an appropriate informed consent process has been followed, participants may indeed wish to maintain ownership of their stories, instead of agreeing to blanket confidentially and anonymity arrangements, an issue that has been put forward within the academic community (Giordano *et al.,* 2007; Grinyer, 2009).

A research project with survivors of IPA, run by the University of Oxford and the University of Bristol, published non-anonymised video recordings of survivors on an online platform called HealthTalk (HealthTalk, 2017), where participants speak about their experience of being in abusive relationships. Bass and Davis (2002, p. 358), in regards to a study with survivors of child sexual abuse, report that *"They [participants] saw identifying themselves as a way to end the secrecy and shame that burden survivors of child sexual abuse. They also wanted, quite simply, to tell their story honestly — to name themselves, their abuser, the place where they lived, the facts of their lives".* Nicolaidis (2002) reports on the production of a documentary, where survivors of IPA were given the option of being anonymous, or not. Documentaries in which survivors choose to waive their anonymity have also been produced (Hall, 2016) and, in fact, many survivors choose to come forward and share their own stories online non-anonymously (Odyssey Networks, 2013).

It was the intention of this PhD project to allow survivors to define the terms of their own anonymity and participation in the research, based on 1) accurate and sufficient information provided in the Participant Information Sheets (Appendix A) and by me, as the researcher, as well as 2) following an appropriate informed consent procedure (Appendix B) that allows participants time to reflect and review their own terms of participation. The scope and limits of this project, however, were redefined through

a lengthy process of ethics review, which has resulted in blanket anonymity for all participants (please see Section 7.2: RQ3 for an in-depth discussion). This, alongside the ongoing academic discussion regarding what constitutes ethical research in design and in participatory research, highlights gaps in the current understanding of ethical best-practice, and in the guidance available to designers-researchers working alongside participants that have experienced trauma. This work aims to contribute to the ongoing work being developed on the ethics of PD and research. Chapters 3, 4, and 5 each contain a section discussing the measures that were put in place in order to ensure ethical practice and safeguard participants within this work. Chapter 3 refers to interviews with participants, Chapter 4 to the codesign workshops, and Chapter 5 to the evaluation of a prototype intervention.

2.2.3 CONCLUSION

The review of socially engaged design, provided in this section, aims to contextualise the selection of codesign as a methodology for engaging survivors of IPA in addressing technology-facilitated forms of abuse. To this effect, a review of design's strengths in addressing *wicked,* ill-defined, ever-changing problems, such as IPA, was provided. Alongside a contextualisation of codesign as a democratically- and politically-engaged movement that privileges the participation of non-users, or non-experts, in the design of the *infrastructure,* services, and products for which they will ultimately be the target-audience. Furthermore, the ever-growing engagement of design with social issues and the sociotechnical work that is necessary to *infrastructure* such projects was also discussed. The *infrastruturing* that was necessary, as part of this particular project, and the engagement with survivors of IPA and support workers is discussed in Chapter 4. Finally, this section concludes with reflections on participant autonomy and anonymity within PD research, followed by a brief discussion of how it impacted participant anonymity and autonomy in this work, as well as how this work aims to inform future development of ethics in codesign. Further discussions on the ethical procedures involved in this PhD project will be detailed in Chapters 3, 4, and 5.

2.3 INTIMATE PARTNER ABUSE AND TECHNOLOGY-FACILITATED ABUSE

This section reviews the problem of technology-facilitated abuse within the frame of IPA — a *wicked problem.* It also identifies the main challenges that inform this work,

which are the foundation for the development of the research activities detailed in Chapters 3 and 4.

2.3.1 INTRODUCTION

IPA is a violation of individuals' fundamental human rights. It can be understood as any behaviour, by an intimate partner or ex-partner, that causes physical, sexual, or psychological harm, including coercive and controlling behaviours (World Health Organisation, 2017).

Westlund (1999) argues that some of the most overt and pervasive methods of exerting power and control over women are domestic and sexual violence, which she refers to as "pre-modern" forms of exerting power in Foucault's definition of "pre-modern" (Foucault, cited in Westlund 1999, p. 1048). In these pre-modern forms of abuse, abusers maintain power over their victims through patterns of coercive behaviour and by instilling the fear of violent punishment for non-compliance with the abuser's demands and expectations. The closeness between the abuser and the victim are distinct from modern structures of power enforced through institutions but rather intrapersonal in nature and therefore classified as pre-modern. The threat of physical punishment means that victims live in fear of the abuser while insults, humiliation, and *gaslighting*[2] gradually wear down victims' mental health and confidence. Furthermore, forced isolation from social networks of family and friends, as well as economic abuse make it extremely difficult for victims to assert their independence or leave the abusive relationship.

Westlund (ibid.) further argues that women subject to domestic violence suffer both from pre-modern and modern forms of violence and oppression. Modern forms include the fact that women often need to resort to modern institutions for help, such as the police, courts, and medical institutions — "[t]hese institutions often revictimize betters women by pathologizing their condition and treating them as mentally unhealthy individuals who are incapable of forming legitimate appraisals of the situations and exercising rational agency over their lives" (Westlund, 1999, p. 1046). One may think of the police and courts as examples of modern institutions where domestic abuse survivors are often disbelieved, not taken seriously, and/or pathologised (Oppenheim, 2019; Bowcott, 2020; Hunter, Burton and Trinder, 2020). However, Westlund (ibid.) also argues that such institutions (e.g., domestic abuse shelters) are essential in supporting women in leaving abusers. Although shelters are places of surveillance where women's

2 *Gaslighting* refers to behaviours intended to make another person doubt their own sanity, memory, and sense of reality. Such behaviours include denying facts and events that took place, purposeful misinformation and contradiction.

movements and behaviour are highly restricted, in many cases they also provide the safety and respite necessary for survivors to access information and support on housing, employment, benefits and finances, custody of children, etc, that will enable them to leave the abusive relationship if they wish to do so. (Westlund, 1999; Sullivan et al., 2008).

In March 2014, the UK government published an action plan to end violence against women and girls, whilst acknowledging that *"[n]ew technology and social media continues to be misused to exploit and target the vulnerable. Bullying, stalking, harassment, and threatening behaviour which occurs online is just as unacceptable as when it occurs offline."* (HM Government, 2014, p. 4). However, although acknowledging novel threats within the landscape of IPA, a 2012 Trust for London report found that 31% of funding to the DA and sexual violence sectors was cut (Towers and Walby, 2012). This led to an average of 320 women being turned away from refuge per day by Women's Aid, due to lack of space. Similarly, statutory provision, including police and court services specialised in DA and sexual violence, has also been significantly scaled down. This trend is one that continues (Grierson, 2018).

Meanwhile, evidence is mounting for the increasing use of cyber-aggression within intimate relationships (Southworth et al., 2007; Schnurr, Mahatmya and Basche III, 2013; Marganski and Melander, 2015; Matthews et al., 2017; Snook, Chayn and SafeLives, 2017). Given the rapid pace of technological development and the fact that frontline support workers are generally not experts in cyber-security and -privacy, along with the impact of funding cuts that ultimately lead to fewer services and less training, this work has identified technology-facilitated IPA as a gap in existing information and support provision.

The following sections define IPA within the context of this work, discuss the effects of IPA, and provide background on technology-facilitated forms of IPA.

2.3.2 DEFINING INTIMATE PARTNER ABUSE

IPA sits within the broader definition of DA, which can include family abuse, honour-based violence, and female-genital mutilation (FGM). However, IPA refers solely to DA between cohabitating or non-cohabitating intimate partners, of all genders and sexual orientations, including physical abuse, sexual abuse, emotional abuse, and financial abuse. Therefore, issues such as honour-based violence and FGM are beyond the scope of this work.

Understanding the dynamics of IPA is crucial to framing the issue. Identifying different types of IPA has implications in court processes, in education, in interventions and measures of success, risk assessment, as well as for policy and legislation. Kelly & Johnson (2008) propose a typology of IPA that looks at individual violent behaviour, within the context of the romantic partnership, and the landscape of control within which the abuse occurs. The authors identify 4 types of IPA: *Coercive Controlling Violence, Violent Resistance, Situational Couple Violence,* and *Separation-Instigated Violence,* which are briefly described below.

Coercive Controlling Violence is identified by the pattern of power and control within which it is embedded. It can involve the use of violence, or the threat thereof. The Power & Control Wheel (Fig. 4), designed by more than 200 IPA survivors, identifies a series of non-violent tactics that are used by perpetrators as part of an ongoing cycle of abuse (Pence and Paymar, 1993, p. 3). Coercive control can be extremely effective and damaging to the victim, even without the presence of physical violence (Johnson, 2010, p. 25). It has recently been acknowledged as a crime in the UK, and is defined as *"a purposeful pattern of behaviour which takes place over time in order for one individual to exert power, control or coercion over another"* (Home Office, 2015, p. 3).

Fig. 4. Power & Control Wheel (Pence and Paymar, 1993)

Violent Resistance occurs when one partner reacts to another's violent or controlling behaviour in a manner similar to self-defence. It generally happens as an immediate reaction to an assault and is intended to protect oneself or others from injury.

In ***Situational Couple Violence***, both partners may be violent, however, violence is not used as an attempt to exert control and fear does not generally occur in *situational couple violence.* Rather, it is often the result of arguments that escalate and partners who have poor abilities in anger and conflict management. It is thought to be the most common type of IPA among married or cohabitating intimate partners.

Separation-Instigated Violence occurs when a relationship ends even though there was no history of violence. It often involves stalking, intimidation, and threats, although neither partner reports being controlled, coerced, or fearful whilst the relationship was ongoing.

This research mainly focusses on *Coercive Controlling Violence, Violent Resistance,* and *Separation-Instigated Violence.* Typologies of violence were born out of the necessity of understanding data regarding gender symmetry and/or asymmetry in DA, that is, whether men or women are more likely to perpetrate IPA. It is often argued that some studies primarily focus on the types of abuse most commonly perpetrated by men, while others investigate the types of abuse that women are also involved in (Johnson, 2010, pp. 2–3), which explains differences in the reporting of prevalence rates according to gender. The following subsection discusses gender and IPA in more detail.

2.3.3 PREVALENCE AND GENDER

One of the biggest issues in the field of DA is the argument over gender symmetry, that is whether males and females are, or not, victims of IPA in equal numbers. Historically, studies conducted by family sociologists, using small-scale representative household samples, have reached very different results than those using data gathered from national crime surveys, shelters, hospitals, and the police, regarding incidence, perpetrator characteristics, severity, and context (Kelly and Johnson, 2008). Studies have employed disparate methods, measurements, and sampling techniques which have produced these different estimates of gender symmetry, or asymmetry, in IPA.

As argued by Kimmel (2002), large-sample prevalence studies have largely relied either on crime victimisation data or on family conflict studies. Crime victimisation studies are generally funded by national, state, and local government agencies. They include

large-scale aggregate data from national household surveys, police data, shelters, and hospitals, and ask about a wide range of assaults, including sexual assault, and assaults by current partners and ex-partners. These surveys generally find significant gender asymmetry, with women being victimised the most. In the UK, according to the Crime Survey for England and Wales (CSEW), 27.1% of women and 13.2% of men have experienced DA since the age of 16 (Fig. 5), which corresponds to an estimated 4.5 million female victims and 2.2 million male victims (Office for National Statistics, 2016). When looking at Crown Prosecution Service (CPS) data, the vast majority of defendants in DA related prosecutions are men (92%). The majority of victims are female (62%), with a smaller proportion of male victims (13%). However, gender was not recorded in more than 1/5 of prosecutions. If this data was excluded, the proportion of victims would be 83% female and 13% male (Office for National Statistics, 2017b). In the context of this work, it is important to note that *"the CSEW estimates do not currently completely capture the new offence of coercive and controlling behaviour",* but there are plans to include questions addressing this for the 2017-18 CSEW (Office for National Statistics, 2017b). Similarly, the CSEW does not include questions related to cyber-stalking, cyber-harassment, or *revenge porn*, within the context of abusive intimate relationships.

Fig. 5. Domestic abuse prevalence rates for men and women in England and Wales (Office for National Statistics, 2016).

On the other hand, when considering family conflict studies, that are based on data from smaller-scale representative household samples, clinical samples, and/or convenience samples based on responses to research advertisements, gender symmetry is generally found. These studies tend to ask about all possible experiences of physical violence, including those that haven't been reported or aren't serious enough to result in injury. However, and contrary to crime victimisation studies, they only ask cohabitating couples and exclude questions regarding sexual assault, placing DA within the context of *"family conflict"* (Kimmel, 2002). Yet, according to the Office of National Statistics (ONS), most DA in England and Wales happens between couples that are not cohabiting or have separated/divorced (Office for National Statistics, 2017a), meaning that family conflict studies may in fact only be focussing on a very limited subset of IPA.

Regarding same-sex relationships, IPA prevalence rates are even harder to accurately estimate. The same methodological, measurement, and sampling issues are present, but aggravated by an historical focus on heterosexual relationships. The gender binary, which assumes the female is the victim, and the male is the perpetrator, as argued by Erbaugh *et al.* (2007), influences the manner in which IPA is regarded in same-sex relationships. For example, as explained by Blumenstein and Guadalupe-Diaz (2016), these cultural constructs have consequences in the way the police may respond to DA, labelling DA between individuals who identify as female as a *"cat fight",* or as a fight between roommates when both individuals identify as male.

This PhD has been informed by crime victimisation data from large national representative samples, where gender asymmetry is found. I have chosen this perspective due to the fact that family conflict studies, that generally observe gender symmetry, do not include data on sexual assault, nor do they consider data from non-cohabitating intimate partners. In this context, participants involved in the interviews and codesign activities are survivors of DA who identify as female, irrespective of sexual orientation.

2.3.4 THE EFFECTS OF INTIMATE PARTNER ABUSE

Women who have experienced DA are at a significantly larger risk of mental health issues such as depression, anxiety, post-traumatic stress disorder and overall poor quality of life (Coker *et al.,* 2000). They are also more likely to experience physical symptoms such as chronic pain, chronic irritable bowel syndrome, STDs, vaginal bleeding, dysmenorrhea, and other gynaecological complications, chronic headaches and neurological damage (Campbell and Lewandowski, 1997; Ellsberg *et al.,* 2008). The extent and severity of the abuse has been found to be directly associated with the severity of mental health symptoms. Additionally, research has found that access to resources has an effect on victims and survivors' mental health, wellbeing and overall quality of life (Beeble, Bybee and Sullivan, 2010). Perpetrators generally use a number of methods — physical threats, intimidation, belittling, and isolation — to restrict victims' access to support and resources. Victims' ability to resist coercive control is limited by access to practical (e.g., money and housing), social (e.g., friends and family), and personal (e.g., self-esteem and determination) resources. Lack of access to these resources impairs victims' ability to leave a relationship, by building emotional and financial dependency on the perpetrator.

Given the current political landscape in the UK, with considerable cuts to DA support services (Towers and Walby, 2012), there is reason to believe that it may have a sig-

nificant negative impact on victims' ability to leave abusive relationships, as well as recover their physical and mental wellbeing (Beeble, Bybee and Sullivan, 2010). Even in cases where victims are able to leave, research has shown that ongoing post-separation harassment, threats, and stalking have serious negative impacts on health and wellbeing outcomes (Campbell and Lewandowski, 1997; Coker *et al.,* 2000; Ellsberg *et al.,* 2008). The nature of digital technologies, including instant messaging (IM), social media, and location tracking, extend perpetrators' reach by enabling them to harass victims remotely and post-separation (Crisafi et al., 2016). It is in this context that the next section discusses technology-facilitated IPA.

2.3.5 TECHNOLOGY-FACILITATED INTIMATE PARTNER ABUSE

Internet-enabled networked technologies collect a wide range of personal data such as geolocation, browsing history, call logs, text message threads, audio and video recordings, social media posts, and in some cases heart rate, physical activity logs, and other biometrics, through individuals' personal devices, work devices, and home devices. The internet-of-things (IoT), which includes wearables, smart home devices, and more common technologies such as smartphones, raises particular concerns for people in abusive relationships, as it is now possible for perpetrators to more easily monitor victims' location and communications, send threats and harassment remotely, as well as expect victims to be reachable and available at all times.

It is well documented that individuals often misuse technology for illegal and/or aggressive purposes (Holt and Bossler, 2015, pp. 6–10). It is believed that the remote character of digital communications leads individuals to become detached from the harmful effects of their actions and words on others (Baym, 2015). Technology as a means of perpetrating abuse and aggression is a growing issue of concern (Grigg, 2010).

In addition to the high-profile cases of gendered abuse taking place in online spaces (see Section 1.1), existing research and feminist discourse also demonstrate that online abuse and harassment is misogynistic and highly gendered (Mantilla, 2013; Megarry, 2014; Vickery, 2018; Rubin, Blackwell and Conley, 2020). Gendertrolling is a commonly used term to describe the participation of numerous, and often coordinated, people in a concerted effort to target women online with gender-based insults and credible threats of murder, rape, and torture (to name only a few) intended to humiliate, instil fear, and silence their targets (Mantilla, 2013). Early writings on computers and the internet believed that the decentralisation, globalisation and democracy of the internet would be equally empowering to all and remove the structural differences that lead to

misogyny, racism, xenophobia, and homophobia offline (Megarry, 2014; Vickery, 2018). However, feminist scholars have long highlighted that the inequalities observed offline migrated to online spaces in both similar and novel formats (Mantilla, 2013; Megarry, 2014; Rubin, Blackwell and Conley, 2020). Mantilla (2013, p. 568) states that "harassment is about patrolling gender boundaries and using insults, hate, and threats of violence and/or rape to ensure that women and girls are either kept out of, or play subservient roles in, male-dominated arenas", which remains the case both offline and online. Although these works focus on harassment online that takes place largely between strangers, technology-facilitated abuse takes on many of the same forms when it comes to intimate partner abuse.

As previously mentioned, the UK Office for National Statistics (2016) indicates the women aged 16-24 are the most affected by DA, whilst those under 30 are the most likely to be engaged with digital communications (Pew Research Center, 2012), which suggests the importance of investigating novel technology-facilitated forms of IPA with female survivors. Within the context of IPA, networked technologies allow perpetrators to further intimidate, threaten, harass, control, demean and stalk victims, beyond the bounds of physical proximity (Southworth et al., 2007; Dimond, Fiesler and Bruckman, 2011; Marganski and Melander, 2015; Freed et al., 2017; Matthews et al., 2017; Freed, Palmer, Minchala, et al., 2018; Chatterjee et al., 2018; Harris and Woodlock, 2018).

The following paragraphs contextualise previous work regarding DA, gender and 1) cyber-stalking, -abuse, and -harassment, 2) stalkerware and hacked or hijacked accounts, and 3) revenge porn, as well as 4) victims' use of technology, within IPA.

CYBER-STALKING, -MONITORING, AND -HARASSMENT

Cyber-stalking often leads to, or is accompanied by physical stalking or the threat of physical stalking either implicitly and/or explicitly (Spitzberg and Hoobler, 2002; Lyndon, Bonds-Raacke and Cratty, 2011). A review of 112 stalking and harassment cases, in the UK, found that 73.2%, included the use of digital technologies — social media, emails, texting and phone calls (Her Majesty's Inspectorate of Constabulary and HM Crown Prosecution Service Inspectorate, 2017). Furthermore, research has found that controlling and coercive behaviours often lead to physical violence and that, female college students who experienced verbal and physical abuse during an intimate relationship, were more likely to be stalked once the relationship had ended (Coleman, 1997). Research on perpetrators of domestic abuse found that cyber-monitoring was positively related to perpetration of physical and/or emotional abuse (Brem et al., 2017).

What is more, a 2016 UK Comic Relief report on technology-facilitated IPA, indicates that 47% of their respondents had experienced some form of cyber-monitoring. A further quarter of respondents said that they did not know for certain if they were being monitored (Snook, Chayn and SafeLives, 2017). These findings are aligned with an earlier Women's Aid study, which found that 45% of victims had experienced technology-facilitated IPA during their relationship, 48% once their relationship had ended, and 75% reported that the police did not know how to respond to novel technology-related threats (Laxton, 2014).

Fig. 6. Prevalence rates for cyber-stalking and –harassment (Her Majesty's Inspectorate of Constabulary and HM Crown Prosecution Service Inspectorate, 2017), and for DA cases with a technology component (Snook, Chayn and SafeLives, 2017).

Within HCI, several authors have begun to investigate the role that digital technologies can play within abusive relationships. Southworth at al. (2007) in a US-based study, reviewed victims' self-reported experiences and news stories from The Stalking Resource Center and the Safety Net Project in an effort to understand how technologies were being used to perpetrate abuse. They 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.

Dimond *et al.* (2011) interviewed 10 survivors in a domestic abuse 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 (2016) surveyed 46 victims and 152 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. Harris and Woodlock (2018) draw on data from 2 Australian research projects, including interviews with 30 victims, as well as focus groups and online surveys with a further 46 victims

and 152 professionals. They describe the quality of *spacelessness* that characterises technology-facilitated abuse. In this sense, perpetrators are able to continue to harass and abuse victims even when not physically co-located. What is more, the instantaneous nature of digital communications enables an immediacy across physical distance that was not possible prior to the proliferation of personal internet-enabled devices.

Matthews at al. (2017) interviewed 15 survivors as part of 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. (2018) carried-out focus groups with 39 survivors and interviews with 50 professionals. They 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 (UI). The UI bound adversary is, therefore, not an IT expert but rather a regular user who interacts with the system through the same UI as the victim. In a separate analysis of the same dataset, Freed at al. (2017) find that survivors and support workers are not confident in their ability to deal with technology-facilitated IPA, lacking the necessary expertise and resources. Similarly, the already mentioned Comic Relief study, also revealed that domestic abuse support workers did not feel confident in supporting victims of technology-facilitated IPA, especially regarding advanced digital privacy settings and needs (Snook, Chayn and SafeLives, 2017). Additionally, research found that prevention advice given by the police, in the UK, is often unsafe and that it may, in fact, increase victims' risk (Her Majesty's Inspectorate of Constabulary and HM Crown Prosecution Service Inspectorate, 2017), as demonstrated by the quote below.

> *"We were also told by victims' groups that police officers sometimes advised victims to change their phone numbers, or not to check their Facebook account. Such advice not only fails to recognise that this may cause the perpetrator to find other ways of offending, but it also does not allow the victim to monitor and understand the nature of the risks that they face and report them." (p. 52)*

STALKERWARE AND HACKED OR HIJACKED ACCOUNTS

Spyware is malicious software designed to access and monitor the activities of a device and covertly transmit that information, over a network, to another device. Stalkerware includes spyware but can also include commercial software designed to keep track of children, and pets, when it is misused to monitor a third-party without their knowledge

and/or consent. It can be installed by having physical access to a device, or remotely, for example, through a hidden email attachment. Depending on how sophisticated the software is, it can allow perpetrators to monitor victims' location, as well as texts, phone calls, emails, account passwords, and browsing history.

Given the relatively recent character of stalkerware, alongside the fact that it is intended to operate covertly, it is hard to estimate how prevalent the phenomenon is. According to a Motherboard investigation of leaked data, tens of thousands of individuals around the world are being monitored through stalkerware without their knowledge (Franceschi-Bicchierai and Cox, 2017). A survey of DA shelters in the US revealed that 85% were working directly with victims who had been tracked, by perpetrators, through their GPS location (Shahani, 2014). More recently, Chatterjee at al. (2018) examined the landscape of intimate partner surveillance apps — spyware — available on app stores, such as *mSpy, HelloSpy,* and *MMGuardian.* They found hundreds of commercially available apps that have either been purpose-built or that can be easily repurposed to monitor an intimate partner without their knowledge.

Even if perpetrators are not using stalkerware, victims are often coerced or forced into disclosing their passwords for accounts such as online banking, social media, and email (Woodlock, 2016; Matthews *et al.,* 2017; Freed, Palmer, Minchala, *et al.,* 2018). Access to victims' passwords has been found to enable perpetrators to hijack accounts and impersonate victims online in correspondence with family and friends (Tokunaga and Aune, 2017), as well as to collect information that can be used as a weapon to threaten victims' reputation (Bocij, 2004, pp. 7–12).

Fig. 7. Refuge victims, in the US, whose location has been tracked by perpetrators (Shahani, 2014).

REVENGE PORN

Revenge porn, or image-based sexual abuse, is generally understood as the creation and/or distribution of private sexual images, by an intimate partner or ex-partner, without the consent of the person represented in the photographs. It is a gendered

form of abuse, with women being the overwhelming majority of victims. This type of imagery is generally posted online on social media and on pornography platforms. It is then routinely reposted and shared across the internet. It is estimated that there are more than 3000 websites dedicated to *revenge porn* alone and the majority of people posting the images are male ex-husbands, ex-boyfriends, and ex-lovers (DeKeseredy and Schwartz, 2016). In this context, *revenge porn* falls within the remit of IPA (HM Government, 2016).

Although statistics on the prevalence of revenge porn are not widely available, 1160 cases were reported, across 31 England and Wales police forces, between April and December 2015 (Laville, 2016). In addition, according to the Government Equalities Office (2015), the revenge porn helpline that was set up to provide specialised information and support to victims dealt with over 280 individual cases within the first 6 months of going live. More recently, an article in the Huffington Post cites a Refuge study finding that 1 in 7 young women have received threats that their intimate photos will be shared without their consent. While two thirds of cases reported to the revenge porn helpline involve women, suggesting it is a form of gendered online violence (Packham, 2020). The real extent of the issue is difficult to assess, especially when recent data from police forces and the Crown Prosecution Service (CPS) are not currently available. I put in a *Freedom of Information* request, to the police forces in London, on the 12th of March 2018, which never received a response. Nonetheless, as a form of gendered technology-facilitated IPA, I have chosen to include revenge porn in the contextual review supporting this work.

VICTIMS' USE OF TECHNOLOGY

This section has largely focussed on the ways technology is appropriated as a tool to propagate abuse. However, technology can also be used, by victims and survivors, to protect themselves, resist the abuse, and seek assistance. Victims and survivors employ a wide-range of tactics to deal with cyber-aggression. These strategies include 1) managing social media privacy, 2) creating online accounts under aliases, 3) *blocking* numbers and online accounts, 4) replacing compromised devices, 5) limiting online communications, including those with friends and family, as well as 6) limiting their own use of internet connected devices (Eterovic-Soric *et al.,* 2017; Tokunaga and Aune, 2017). These are strategies that often lead to excessive monetary costs involved in replacing devices, isolation from family and friends, as well as economic and social disadvantages related to limiting their use of the internet.

On the other hand, Melander (2010) reports on victims using social media to end a relationship with a perpetrator, and as a way of voicing their opinions without fear of immediate physical aggression. Tokunaga & Aune (2017) describe victims using digital communications to confront intimate cyberstalkers and to call them out on their behaviour. Southworth (2007) found that victims often seek information and support online, and online information is also used to plan escapes from an abusive relationship (Snook, Chayn and SafeLives, 2017), even though a significant proportion of the information available to victims has been found to be contradictory, scattered, and hard to digest (Snook, Chayn and SafeLives, 2017).

The current landscape of information and support provision, in the UK, regarding technology-facilitated abuse has not been able to keep up with technological progression. A reactive approach to dealing with abuse through widespread technologies, such as social media and smartphones, has meant that victims are needing support before professionals are equipped to respond. Similarly, existing research has mainly focussed on current widespread technologies and the issues that victims are experiencing in the present. This work aims to extend existing research by using codesign methods alongside survivors and support workers in anticipating and preparing for the near-future threats posed by shared smart home devices. Accordingly, the next section discusses issues of smart homes and interpersonal privacy.

2.4 THE FUTURE, SMART HOMES, AND INTERPERSONAL PRIVACY

The increasing embedding of IoT devices into "smart homes" poses a near-future threat to victims of IPA, as do wearables that track users' locations and biometric data. Currently, consumer IoT devices — smart door locks, thermostats, activity monitors, smart watches — connect to users' smartphones as a central point of control. If perpetrators have access to victims' phones, they have access to data from a potentially wide range of devices that allow them to track almost every aspect of a victim's life. Furthermore, future scenarios for *smart homes* envision *smart hubs* — Amazon Echo, Google Home, Apple HomePod, Samsung Connect Home — as being the central devices that allow users to manage all functionality in a networked house. However, current smart home devices do not offer robust support for multiple user accounts, leading to scenarios in which all people living in a home have access to everything on the account used to activate a given device (Jang, Chhabra and Prasad, 2017).

Furthermore, a number of proposals for a social internet-of-things (SIoT) have emerged in recent years. What these proposals envision is a network of devices and people, in which devices can become "friends" with other trusted devices. For example, in the scenario of an intimate relationship, individuals' devices could autonomously share information, with each other, and receive privileged access rights if their devices detect long-term frequent interactions between the owners. The vision for social smart objects is they will be able to 1) communicate with other objects in an autonomous way and independent of their owners, 2) autonomously crawl the network of devices and build "relationships" with devices capable of providing data or a particular service, and 3) advertise their presence and the services they are capable of providing to the rest of the network (Atzori, Lera and Morabito, 2014). Although this may not be seen as an issue for the general public, it could become very problematic for victims of IPA, which account for 27.1% of women and 13.2% of men in England and Wales (Office for National Statistics, 2016). In this scenario, it is easy to imagine the several added layers of complexity that would be required for everyday consumers to manage their digital privacy and security. Especially given that users, who are not under the pressure of living with an abusive partner, are currently unable to effectively manage the complexity of existing security and privacy settings (Acquisti *et al.,* 2017).

The section provides a brief background and definition of smart homes. It then discusses existing smart home research in relation to the gendered dimension of home living, followed by a discussion of interpersonal privacy — or privacy between individuals — within the context of shared home devices. The work discussed in this section relates to the findings presented in Chapter 3 and 4.

2.4.1 INTRODUCTION

Smart home device adoption rates in the UK are currently around 19.7% and expected to reach 39.0% by 2022 (Statista, 2018b). Revenue from smart home technologies is expected to be around £118,799m in the UK by 2023 (Statista, 2018b). Although wide-spread adoption has not been as rapid as initially expected, technology giants, such as Amazon and Google, have been releasing an increasing amount of smart home devices in a reaction against an oversaturated smartphone market and in a push to find new revenue sources (Shin, Park and Lee, 2018). What is more, governments all around the world are funding *smartification* projects based on a widespread belief that smart cities and smart homes are able to maximise energy efficiency and, therefore, contribute to a reduction in fossil fuel consumption and climate change (European Commission, 2016;

Vesnic-Alujevic, Breitegger and Pereira, 2016). The concept of a smart home is based on the notion that an internet-enabled intelligent agent, through a series of smart devices, can perceive the state of the physical environment and its inhabitants. Based on the perceived states, the agent is then able to automatically make adjustments to assure residents' safety and comfort, as well as assisting them in achieving daily tasks such as cooking, scheduling, and maximising household energy efficiency (Cook, 2012, p. 1579).

Early 1980s visions of the smart home promised more leisure time by reducing the effort involved in housework, particularly for women (Nyborg and Røpke, 2011; Strengers, 2016). While traditional household appliances such as the vacuum cleaner and clothes washer did, in fact, reduce the amount of physical effort required for such tasks, they also created more work for women by raising expected social standards of cleanliness and reducing the perceived effort of maintaining a household (Strengers and Nicholls, 2018). At the same time, women have taken up work outside of the home. Both of these factors contribute significantly to women's paid and unpaid labour. I choose to say "women" here and not "people" due to the fact that most of the housework, even in "developed" countries, is still mainly performed by women (Perez, 2019). What is more, the types of work performed in the home are largely defined by gender norms (Giménez-Nadal, Mangiavacchi and Piccoli, 2019; Perez, 2019). Therefore, in order to understand the context of use of smart home devices, it is essential to understand the dynamics of the household. Given that this work focusses on female victims of domestic abuse, and that all of the research participants were involved in an abusive relationship with a member of the opposite sex, it is essential to understand the household dynamics that playout between women and men within the context of a *smart* home.

The remainder of this section discusses, in turn, existing research and theory related to 1) *smart homes, the domestication of technologies, and gender,* as well as 2) *smart homes and interpersonal privacy.*

2.4.2 SMART HOMES, THE *DOMESTICATION* OF TECHNOLOGIES, AND GENDER

Although a growing amount of industry and academic work focusses on smart homes, it has mainly concentrated on the technical challenges of development, whilst overlooking social aspects of home living and the complexity of relationships between household members (Wilson, Hargreaves and Hauxwell-Baldwin, 2015). Smart home development has largely assumed that if a particular technology works and is available

to consumers, it will be adopted. However, a multiplicity of factors influence technology adoption and the way that technologies are used in daily life, which may not correspond to developers' and designers' intentions for how a given artefact will, in fact, be used.

Strengers at al. (2019) argue that technological determinism has largely shaped the development of technologies meant for the home, whilst overlooking the social structures that shape technology usage within a domestic setting. In opposition to technological determinism, is *domestication* theory. *Domestication* theory opposes the view that technologies are pre-given, unchanging entities that diffuse through society and are adopted by *passive users* who 'simply adapt to what is offered to them' (Lehtonen, 2003). *Domestication* theory believes that there is active work, on the part of users, in 'taming' technologies and adapting them to the domestic environment (Hargreaves, Wilson and Hauxwell-Baldwin, 2018). To simplify, *domestication* involves the following cyclical and mutable processes on the part of users:

- being exposed to a new technology, its features, and functionality, as well as reflecting on how it may be useful;
- purchasing and learning how to use the new technology;
- incorporating the technology into everyday life and identity formation, which changes over time and can also result in rejection or processes of re-domestication (Sørensen, 1994).

In this context, it can be argued that the *domestication* process involved in living with smart home technologies may not be experienced by all household members in the same way. The social structures, effects of the technologies, adaptation strategies, and perceived benefits and trade-offs vary across individuals. Whilst smart home manufacturers promote ideas of reduced housekeeping effort and more leisure time, improved security, and comfort (Hazas and Strengers, 2019) afforded by smart devices, these benefits may not be equally distributed amongst all members in a household. In fact, recent human-computer interaction (HCI) literature highlights that, on the one hand, smart home technologies are intended for the home, where dynamics between household members are highly gendered and their experiences of home living are heterogeneous (Rode and Poole, 2018; Strengers *et al.,* 2019). While on the other hand, a gender dimension is largely absent from HCI studies and theory (Rode and Poole, 2018).

Early work by Berg (1994) argued that the smart house is a gendered construction made by men, from a male perspective, whilst overlooking the meaning of the home from a

female point-of-view. Indeed, smart home devices are largely produced by an industry lacking in gender diversity (and diversity more generally) (Wachter-Boettcher, 2017), which has foregrounded technically proficient and hobbyist men as the target-users and adopters of smart homes (Strengers and Nicholls, 2018; Strengers *et al.,* 2019). As a consequence, it has been argued that women sometimes choose to actively reject novel technologies, present themselves as non-technical, or experience what has been termed as *gender inauthenticity*. *Gender inauthenticity* refers to a misalignment between feminine gender identity and displaying technical competency (Ensmenger, 2015).

Unsurprisingly then, research has found that the use of technology within the home mirrors and reinforces stereotypical divisions of labour and gender roles. On the one hand, more work is created for men in the form of purchasing, installing, and maintaining smart devices — *digital housekeeping* (Rode and Poole, 2018; Strengers *et al.,* 2019). On the other hand, women's chores remain largely the same and may, in fact, be exacerbated due to the time that men are now spending on *digital housekeeping* (Strengers *et al.,* 2019). Rode and Poole (2018, p. 8) found that, more often than not, men play the role of technology czars within a household, while women play the roles of *"the good woman, damsel in distress, and technophobe".*

Their study of 29 households in the United States (US) revealed that, in the majority of cases, men were responsible for installing, maintaining and operating smart home devices (Rode and Poole, 2018). Particularly relevant to this PhD work is the authors' discussion of *digitally chivalrous gentlemen* and *helpful* men, in which the adult man in the household assumes the role of installing, maintaining, and controlling technology in an effort to remove this burden from his female partner. The authors discuss this as a form of *digital chivalry* in which men position themselves as using smart home technologies, such as digital doorlocks and indoor cameras, to care for and protect the family. However, Rode and Poole (ibid.) also argue that men's control of technologies within the household can have the result of limiting women's mastery of such devices and leave them vulnerable in cases of temporary and/or permanent separation from the technology *support provider.* This could happen, for example, in the case of a divorce where one of the partners may find herself living in a home that she does not know how to operate, nor does she have the necessary system permissions to do so.

Similarly, in a study of 18 households in the US, Geeng & Roesner (2019) observed differences in power, agency, technical skill, and technical interest among different members in a household. In 16 of the households, it was the male who assumed the

role of technology *driver;* and 14 of the *technology drivers* were the only occupants who had installed any sort of smart device in their homes. The *drivers* often had a female partner who assumed the role of the passive user. The authors argue that, in this context, smart home *drivers* have access to more functionality and information than *passive users,* which allows them to set permissions for different household members and know when someone is, for example, in or out of the house. What is more, when improperly used, privileged access to functionality and information can enable the surveillance of other household members without their knowledge or consent (Geeng and Roesner, 2019).

A 2019 study of 31 Australian homes revealed that, in most cases, *"masculine-identifying tech-enthusiasts"* were responsible for purchasing, setting up, and maintaining digital devices in the home (Strengers *et al.,* 2019). The study's authors observed traditional gendered divisions of labour in the household and that the *digital housekeeping* work was mainly undertaken by men — an activity that was quite often seen as a pleasurable hobby. One of the challenges highlighted in their work is that of *"overcoming potential threats to women posed by increased security, surveillance and control in the home",* which is a direct result of the gendered control of networked technologies within the households they observed (Strengers *et al.,* 2019).

Despite the fact that family units are quite often idealised in HCI literature and smart home promotional materials, families are not always healthy, happy, and caring units (Munro, 2018). In cases of intimate partner abuse (IPA), for example, one partners' control over home technologies may enable intimate surveillance without the victim's knowledge and/or consent. It is important to note that, as previously mentioned and despite the studies cited above, sociological work on smart homes has largely been absent from HCI and other related literature (Wilson, Hargreaves and Hauxwell-Baldwin, 2015). A recent review of smart home literature found only 20% of publications were based in the social sciences, rather than in technical development (Wilson, Hargreaves and Hauxwell-Baldwin, 2015). Furthermore, as highlighted by Strengers (2016), studies that include users have mainly focussed on user-acceptance of smart home devices and on how such devices can respond to user-needs. Less attention has been paid to how smart home devices interact and influence the domestic environment and its routines.

Technology-facilitated abuse sits within the broader context of gender inequality and the traditional male-dominated digital technology industry and therefore, the interaction between smart home devices and the power dynamics of the domestic environment

cannot be ignored. This work aims to extend existing research on the social dimensions of smart homes. This research with IPA survivors and support workers contributes to an understanding of user needs and requirements beyond the male, middleclass, early-adopter. It, therefore, contributes by bringing in a perspective that has not been considered before in smart home theory, design, and development. In light of a gendered dimension in the control of smart home devices, the next section introduces issues of interpersonal privacy between household members in a smart home.

2.4.3 SMART HOMES AND INTERPERSONAL PRIVACY

Devices within the home, such as smart door locks and indoor security cameras, gather a wide range of information regarding household members' habits and routines. Information about a household member's daily activities can be gathered through device logs (e.g., a door lock will have information on when a user left and re-entered the house) or through live video and audio feeds, which can be accessed remotely, in real-time, by another user outside of the house. Although such capabilities may not be of concern to all users, access to shared home device feeds and logs can be problematic in households where abuse is taking place.

Smart home privacy and security research has mainly focussed on the technical aspects of insecure software engineering practices and user privacy from service providers and manufacturers (Wilson, Hargreaves and Hauxwell-Baldwin, 2015; He *et al.,* 2018; Zheng *et al.,* 2018). As argued by He *et al.* (2018), less attention has been directed at investigating who has control of shared home devices and in which contexts, as well as ways of authenticating different users within the same household.

Traditional devices such as laptops and smartphones are personal devices — intended to be used solely by one person — and therefore, once a user is authenticated there is less of a need to continually verify who they are and what they have access to. Furthermore, whilst personal devices have screens or keyboards that can be used for password and biometric authentication, many smart home devices are shared between users and lack these forms of input. Hence, such forms of authentication are no longer an option for smart home devices. In fact, smart home devices are notoriously poor at supporting multi-user accounts (Jang, Chhabra and Prasad, 2017). The result is that, more often than not, the user who sets up the devices in the home has access to shared data logs, remote feeds, and the ability to constrain other users' permissions to access a device (Mennicken and Huang, 2012; Mäkinen, 2016; Rode and Poole, 2018; Geeng and Roesner, 2019; Strengers et al., 2019).

Interpersonal monitoring — monitoring between individuals — within a household raised concerns even before the proliferation of smart home devices. In an early effort to understand what might affect people's perceptions and use of home sensing and recording technologies, Chloe *et al.* (2012) conducted an empirical study with 11 households in Seattle, United States. The study included in-lab activities, the use of sensor proxies in situ over a period of 4 weeks, and interviews with participants. It was found that tensions arose, regarding privacy and acceptability of sensing and recording technologies in the home, between members of the same household. The authors report on tensions between couples, between parents and children, as well as between residents and visitors. They found that, for example, couples were concerned over recordings 1) being used by one partner to verify the veracity of events as recounted by the other partner, or 2) being taken out of context and used within divorce and child custody proceedings.

Similarly, Mennicken & Huang (2012) conducted a study investigating user motivations in adopting smart homes, the phases involved in making a home smart, and the roles that were carried-out during adoption and use by individual household members. The authors conducted semi-structured interviews with participants from 7 households living with smart home devices, 3 households in the process of building a smart home, and 7 professionals working on smart home development. All primary users — or *technology drivers* — in their study were male, whilst all *passive users* were female, supporting the studies reported on in the previous section (Rode and Poole, 2018; Geeng and Roesner, 2019; Strengers et al., 2019). What is more, although their study was not specifically focused on issues of interpersonal privacy between household members, the study nonetheless uncovered cases of the primary user denying access permissions to all other users in the same household. Power over which permissions are assigned to other household members essentially gives the primary user control of the system and access to all household data, including data gathered from other household members.

In a more recent study including 13 interviews with users of smart home surveillance devices, one of the observations was that if devices offer affordances that enable surveillance (e.g., video and audio), then there are users who may not trust themselves to resist monitoring other household members (Mäkinen, 2016). Many of the study participants report monitoring other household members, especially children or adults engaged in a potentially dangerous activity, out of care. Whilst caring surveillance was accepted as beneficial by all participants, Mäkinen (2016) highlights the fine line between surveillance as an act of caring or surveillance as an act of control. Interestingly, in

Jakobi *et al.* (2017), an 18-month living lab study of 14 households, only once users had been interacting with smart home devices, for a period of time, did they realise their potential for surveillance in the amount of information that could be derived about a household member through historic device logs. For example, participants realised that such data could be used to infer when someone was at home or not.

Goulden *et al.* (2018) propose that networked home technologies play an important role in when and how the activities of others can be observed within the household. Based on a study of 6 households, they argue that this leads to new forms of observability, which, in turn, creates new forms of accountability as activities that were previously hidden are now made visible through smart device data. The visibility of previously unseen behaviours can be mediated through direct visualisation of centralised home device logs, feeds, or through the adaptive behaviour of the system itself. What is more, these new forms of observability mean that household members require novel ways of managing their privacy or regulating their behaviour when privacy is no longer possible (e.g., leaving the house without being logged by the smart door lock).

In another study, Tolmie and Crabtree (2018) point out that when data is accessible through shared devices, one user's effort to keep the data hidden may be an act that, in itself, becomes accountable and questionable by their partner. The authors give an example of one partner, every night, asking the other *"are you off to bed now?"* and only then checking their Facebook page on the shared tablet, which over time is a behaviour that could be interpreted as *suspicious.* In the case of IPA, if a victim chooses to put a device, such as an indoor security camera, on *"snooze"* mode so that it doesn't record for a period of time, then this may be questioned by the perpetrator. In such a scenario, the act of seeking privacy is recorded on the shared device log and open to be viewed and questioned by the primary account holder. Centralised and aggregated device logs, thus, remove a layer of interpersonal privacy between household members in a smart home. What is more, it may not always be the case that all household members understand and consent to the removal of that layer of privacy, prior to device adoption. It may be the case that the primary user installs smart devices and other household members only become aware of the devices' impact on privacy through daily usage. At which point it may be too late to request that the device be removed without generating conflict.

In this context, a study being run collaboratively between PETRAS IoT Hub at University College London, the London Violence Against Women and Girls (VAWG) Consortium,

and Privacy International has found that although IPA through the IoT is not yet widespread, these technologies show the potential for exploitation, especially regarding shared accounts, tracking/location capabilities, and remote audio and video feeds (Velia, 2018). The researchers report concerns over surveillance through devices logs on smart home hubs (e.g., the Amazon Echo), smart thermostats, as well as over the remote control of devices that could be used to, for example, deprive a victim of heating during winter. Their study has been informed by interviews with domestic abuse organisations, frontline support workers, police representatives and academics in the UK.

Other authors have acknowledged the need for participatory approaches to smart home development. Rohracher, already in 2003, argued that engaging with a wide range of potential users may be an effective approach to ensure that the widest possible range of user needs, concerns, and requirements are addressed in smart home design. The author also highlights that research on smart homes, when it does involve users, they tend to belong to specific social groups comprised of early-adopters who are relatively wealthy and highly educated (Rohracher, 2003). However, as noted by Strengers *et al*. (2019), users have largely been absent from smart home research and development. More specifically, individuals from marginalised populations are less likely to participate in research on networked technologies, resulting in a situation in which researchers and manufacturers are unaware of the risks that such technologies may pose to, for example, victims of IPA (Zheng *et al.,* 2018). Further research on the impact of smart home devices on interpersonal privacy within the home is necessary to avoid empowering those using devices for abuse and placing victims at further risk.

This PhD work contributes to a more comprehensive understanding of a more diverse set of user needs, concerns, and requirements regarding smart homes and interpersonal privacy. More specifically, it aims to add the voice of a marginalised group, for whom reduced interpersonal household privacy may lead to escalations in abuse and violence, to the HCI discourse and to the design of near-future smart home devices.

2.5 CONCLUSION

The contextual review has informed this research in a number of ways and layers the foundation upon which the aims and objectives of the research (Section 1.3) can be addressed, as informed by existing work and the context within which this PhD sits. Firstly, DA gender prevalence studies set the scene for this work's focus on recruiting survivors of DA who identify as female. Secondly, recent research points to the fact

that cyber-aggression has become a tool for perpetrators to further harass, control, and intimidate victims. It therefore poses a novel threat within the landscape of DA and is identified as a gap in current knowledge and support service provision. Although existing and ongoing research is investigating forms of cyber-aggression within IPA (Matthews *et al.,* 2017; Snook, Chayn and SafeLives, 2017; Freed, Palmer, Ristenpart, *et al.,* 2018), this work builds upon those studies by, as described in Chapter 3, including novel sources of data (online domestic abuse forums), as well as interviews with survivors and support workers. Finally, accounts of IPA facilitated by smart homes devices have begun to emerge (Bowles, 2018) and given their relatively novel nature research has yet to investigate issues of interpersonal privacy in smart homes within the context of IPA. The codesign workshops with survivors and support workers, reported on in Chapter 4, adopt a speculative approach to predicting the interpersonal privacy threats posed by these technologies to victims. The aim of this work is proactively anticipate such threats and provide victims and support workers with the tools necessary to understand the issue and safeguard themselves. The tool that has been developed, in collaboration with Refuge is detailed in Chapter 5.

3

GATHERING INSIGHT: INTERVIEWS & FORUM DATA

A growing body of research has investigated the role of digital technologies within abusive intimate relationships. Much of this research has found that email, social networks, and mobile phones are used by perpetrators to monitor, harass, threaten, and intimidate victims remotely and on an ongoing basis (Southworth *et al.,* 2007; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Chatterjee *et al.,* 2018; Harris and Woodlock, 2018). Technology-facilitated intimate partner abuse (IPA) has several characteristics that differentiate it from in-person IPA. As argued by Watkins *et al.* (2016), the nature of digital technologies allows perpetrators to harass and monitor victims remotely, regardless of physical distance, and therefore enable the abuse to permeate into victims' lives at any time and in any space. Furthermore, technology-facilitated abuse lacks the social and physical cues that characterise in-person communication, therefore, perpetrators may be less inhibited and send content that is more abusive than what they would otherwise communicate face-to-face. Finally, the relative permanence of digital communications means that they can be read more than once and can be shared with a larger audience (e.g., *revenge porn*) (Watkins, Maldonado and DiLillo, 2018).

Research on technology-facilitated IPA has mainly been conducted in the US (Dimond, Fiesler and Bruckman, 2011; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017) and Australia (Woodlock, 2016; Harris and Woodlock, 2018) with support workers and victims engaged with professionalised support services. However, little is known about the current landscape in other geographic regions and about victims who may not be accessing formal support. In this context, a study of data from three peer-to-peer online domestic abuse forums was conducted. The forums are open to any victim or survivor that wants to join, regardless of whether they are accessing formal support or not. Interviews with survivors and UK-based support workers were also conducted in addition to the analysis of online forum data, in order to gain perspective into the current support provision landscape in the UK. In this context, this study aimed to answer the following questions:

1 Are the current forms of technology-facilitated IPA being faced by survivors who are not engaged with formal support services, the same as those reported by existing research in the US and Australia?

2 Are the challenges faced by UK-based support workers, in providing support, the same as those reported by research in the US and Australia?

The findings from the *insight gathering* phase reported on in this chapter, have been used to inform the codesign workshops discussed in Chapter 4. This chapter describes the processes of gathering forum data, conducting interviews, and analysing the data. It then reports on the main findings and offers a discussion of those findings. The chapter closes with a conclusion that outlines how the findings from the interviews and forum data informed the codesign workshops.

3.1 INTERVIEW PROCEDURE

Semi-structured interviews are often considered to be an effective way of giving voice to marginalised or under-researched communities (Willig and Rogers, 2017). In this work, semi-structured interviews were conducted with survivors of IPA and professional support workers. The interviews explored 1) their experiences of technology being leveraged, by perpetrators, as a tool for abuse; 2) strategies used to cope and defend themselves from the technology-facilitated abuse; 3) gaps in support and information provision; as well as 4) needs for improving existing support services. Interviews with survivors were either conducted over video conference calls or at a trained therapist's office. Interviews with professionals took place either remotely or in a private space within their work premises. Professionals were authorised to take part during their regular working hours. In addition to the questions asked to survivors, professionals were also asked about their digital security and privacy knowledge, as well as thoughts on and needs for future training. These questions were asked in order to identify gaps in existing support provision. Interviews lasted between 30-95 minutes, depending on participants' availability. All anonymisation and consent procedures were discussed with interview participants. Participants were also made aware that they could revoke their participation at any point without negative consequences.

3.2 FORUM DATA SCRAPING PROCEDURE

Regarding forum data, web scraping[1] was used to retrieve posts from three online domestic abuse forums, and then exported in JSON. An automated scrape of 200 pages was run for each forum, resulting in:

1 Web scraping is the process of collecting structured web data in an automated fashion. For this PhD, forum pages in HTML were scraped and exported as JSON (JavaScript Object Notation) files for analysis.

- 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. I 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, in an effort to preserve forum members' anonymity.

3.3 PARTICIPANT CHARACTERISTICS

Four female domestic abuse survivors [S] were interviewed, two were based in the UK and another two in the US. Three survivors had children with the former abusive partner and none of them were currently in a relationship with the former abusive partner.

Nine support workers [SW] were interviewed and are all based in the UK. 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 both victims and perpetrators on violence prevention programs. All participants' names have been replaced with a pseudonym. Regarding forum data, it is not possible to provide demographics, as most forum users login under a screenname and do not share identifying information.

3.4 ETHICS

In order to reduce possible risks of participation, only survivors who were no longer in an abusive relationship were recruited to take part in the interviews. Furthermore, a therapist with experience of supporting victims of IPA was present in all interviews with survivors. The therapist was there to intervene in the interviews should survivors need support, which did not happen in any of the interviews. Interviewees were also

informed that the therapist would be available to them for a session after the interview, free of charge, should the interviews bring up anything they would like to talk about. The therapist was available to meet survivors in-person at her office, or over the phone.

Participant Information Sheets and Consent Forms were sent to participants at least one week in advance of interviews. First contact with survivors was always achieved through a support organisation or group, rather than directly by me. This was done in order to preserve potential participants anonymity until they had agreed to take part. Once survivors had agreed to participate, direct contact was established in order to schedule a time and date that suited everyone.

I undertook training on how to support victims of IPA through my volunteering with Victim Support and the Domestic Violence Intervention Project. I began my volunteering activities before the PhD started and have continued throughout, supporting victims of IPA on a weekly basis.

3.5 INTERVIEW & FORUM DATA ANALYSIS

All interviews were transcribed prior to analysis. A thematic analysis (Saldana, 2015) 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-enabled abuse. The excerpts were selected following a thematic analysis, which began by a close reading of the interview transcripts. For the forum data, this was achieved through a keyword[2] search method followed by a close reading. Whenever a particular keyword was found, the whole forum post was read, coded, and a transcript saved. An initial phase of coding was carried-out based on a first reading of the data. Codes were then iteratively defined and described through a second close reading. The codes were documented in a codebook that was used to perform an in-depth analysis of the data, which was subject to a third and final round of coding. Lastly, a thematic grouping of the codes led to the themes detailed in the *Findings* section below.

Interviews with survivors were analysed in conjunction with the forum data. Given that only two survivors were based in the UK, it was not possible to focus the analysis on UK-based survivors' experiences. Contrastingly, interviews with support workers

2 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.

were analysed separately and focussed specifically on the current landscape of UK support provision.

3.6 FINDINGS

This section is organised according to the three main themes that emerged from an analysis of the data, namely:

1. Forms of technology-facilitated abuse;
2. Victims' use of technology within the context of IPA;
3. Peer-support and professional advice on digital privacy and security.

Each theme is composed of two to four subthemes. Table 1 provides an overview of the themes, a description of each subtheme, and illustrative transcripts. It is important to highlight that these three themes are not mutually exclusive and, in fact, often overlap with each other. The following sections expand upon each of the themes in more detail.

THEME 1: FORMS OF TECHNOLOGY-FACILITATED ABUSE

The first theme focusses on the forms of technology-facilitated abuse discussed in the interviews and on the forums. An analysis of the transcripts revealed that a combination of abusive techniques is generally employed by perpetrators, which means that the forms of technology-facilitated abuse described in this section often overlap with each other, as well as being part of a larger pattern of physical, sexual, and/or emotional abuse. For example, in the transcript below, a forum member describes how digital surveillance led to verbal and physical aggression.

> *My abusive partner used variations of monitoring and surveillance apps to invade my privacy and to justify physical assaults against me. The monitoring and surveillance often lead to verbal and physical assaults. I contacted [name of support organisation removed] but because I am not a resident in that country, they cannot offer me practical forms of support.* [CF]

Given the complexity of Theme 1, it has been broken down into four subthemes, namely 1) overt surveillance, 2) covert surveillance, 3) restrictions to device access, and 4) threats, harassment, and abuse. Although there is overlap between subthemes, this has been done for the purposes of clarity and structure.

OVERT SURVEILLANCE

Surveillance was widely discussed among forum members and in the interviews. Overt surveillance, where the victim is aware of being monitored, was the most commonly discussed. The nature of intimate relationships means that perpetrators are often able to gain access to victims' devices and accounts, either because they know or can guess the victims' passwords or by forcing the victim to give them access. In the transcript below, a forum member describes the perpetrator threatening to destroy her devices unless she gives him her passwords.

> *I live with my husband and two children. My husband never leaves home, he also won't agree to end the relationship. He becomes abusive whenever I mention any of these things. He also takes my phone, tablet, etc., and threatens to break them unless I give him my passwords.* [NGOF]

In other cases, perpetrators buy and set up all the devices in a household, giving themselves access permissions to victims' devices. With the emergence of the cloud and the possibility of automatically backing up devices to a central storage location, this can mean that perpetrators only need a single password to access victims' personal information and communications.

> *He bought all our devices! He set all our devices to upload everything (contacts, messages, etc.) to the cloud, which he owns and has a password for. He would get copies of all my emails, appointments, etc.* [NGOF]

Having access to victims' devices and accounts means that perpetrators can monitor activities such as victims' location, movements, and digital communications. Particularly, overt surveillance restricts the ways in which victims can access support. The quote below demonstrates one victim's difficulty in getting in touch with a support worker, which led her to seek support online on the forum.

> *I wish I could call the support worker back but I am at home. He is sleeping, but I only have my mobile phone and the landline phone, and he has access to both of these.* [CF]

In addition to restricting victims' access to professional support, overt surveillance also limits victims' ability to seek support from friends and family. The following transcription illustrates how surveillance forces victims into isolation from their closest social connections and creates an environment stripped of the privacy required to access support.

> *He has access to all my emails, my bank account, my phone. Literally everything. Every time I try to get advice from friends or family, he goes through my messages. Now I delete everything. Even this forum post is sent from an email address he doesn't know about using a browser without trackers. I have no privacy and I am always being watched.* [CSF]

Another victim describes how the perpetrator read text messages that she had exchanged with a friend. In the messages, she seeks support and expresses discontent with the intimate relationship. The forum member reports that the perpetrator became physically aggressive and broke the victim's phone, after reading the texts. Incidents such as this — where digital surveillance leads to physical assault — may have the effect of deterring victims from reaching out for support again.

> *He wanted to read my text messages. I explained that none of them were sexual, romantic, or flirtatious in nature, but I did have some texts complaining about our relationship with a friend. This led him to smash my phone into pieces. He then choked me.* [NGOF]

Furthermore, transcripts reveal that perpetrators will attempt to justify abusive behaviour by claiming that the victim is being unfaithful or intending to do so. Victims' digital communications and social media activity are carefully monitored for any interactions that could be perceived as a threat to the romantic relationship. As one victim describes,

> *He linked himself to my Amazon account so I cannot buy that book [about understanding abuse] online without him knowing. He also checks my online activity and asks about who I may have been talking to. He goes through my Facebook posts and asks me about every man that has left any type of comment: "Who is he? How do you know him? Has he ever been inappropriate?"* [CF]

What is more, as exemplified in the transcript below, perpetrators will leverage allegations of infidelity to enforce further surveillance. In this way, perpetrators' position surveillance as a reaction to victims' behaviour. Behaviour which is framed as antagonistic to the romantic relationship and, consequently, in need of being monitored.

> *After 3 or 4 months together, I started noticing that he checked my phone and email regularly. He lost control over an innocent text that I received from a male friend. He implied that he would put cameras in the bedroom because he didn't believe me when I told him that I did not know why there was a pillow on the floor.* [CSF]

Most of the above examples of overt surveillance rely on perpetrators having physical access to victims' devices in order to carry out surveillance. However, even without

Theme	Subtheme	Description	Example quote
Forms of technology-facilitated abuse	Overt Surveillance	Surveillance refers to perpetrators monitoring victims in a number of ways, such as tracking their location and/or reading their IMs, emails, etc. Surveillance is overt when the victim is aware of being monitored.	*He will go through my phone to check that I'm not flirting with other boys. He also checks my Facebook and Instagram.* [CSF]
	Covert Surveillance	Covert surveillance describes scenarios in which victims are not aware of being monitored or suspect they are being monitored but cannot prove it.	*Is anyone else findings this forum slow to load? It seems very slow to me. I understand if that is normal but I'm paranoid that he's installed tracking software. I am very scared that he will find my posts on this forum.* [NGOF]
	Physical Restrictions to Devices	Refers to the ways in which perpetrators limit victims' access to devices in order to restrict their access to support.	*When I told him that I was going to call the police, he took all the phones and left me in the room.* [NGOF]
	Threats, Harassment, and Abuse	Describes how perpetrators leverage technology to continually threaten, harass, intimidate, and otherwise abuse victims.	*If he continues sending me texts, even after the harassment warning has been put in place. What else will he do? He's already shown that he's capable of nearly killing me.* [CF]
Victims' use of Technology	Evidence Gathering	Evidence gathering refers to victims' gathering digital evidence of abuse for 1) legal purposes or 2) for reminding themselves of perpetrators' behaviour.	*You may need a restraining order to keep safe. I needed one. To get a restraining order you will need proof of the abuse. Save all the threatening texts and emails, do not delete them. Take screenshots of anything that contains threats or verbal abuse.* [CF] *I've started recording him speaking to me. I've also started writing things down because I find that I can't always remember what he has said and done. I feel like I sometimes dissociate.* [CF]
	Social Media	Refers to the ways in which victims are using social media within the context of IPA.	*I went on social media, found his ex-wife and sent her an apology for having been "the other woman". Turns out he was also abusive to her and keeps being abusive long after their divorce. We're friends now and we talk often on social media.* [CF]

Peer-Support and Advice on Digital Privacy and Security	Covering Digital Footprints	Refers to advice being exchanged on the forums on how to cover one's own digital footprints.	*Make sure you wipe your internet history. Don't use passwords for this website that he can guess. Hopefully, he doesn't have spyware on your laptop but, just in case, use a computer that isn't in the home.* [CSF]
	Hacked or Hijacked Accounts	Describes advice exchanged on the forums on how to deal with hacked or hijacked accounts.	[In response to a thread about a hacked email account] *Change the password. Maybe change your email address too. I did and it gave me a lot of peace of mind.* [NGOF]
	Spyware	Describes advice exchanged on the forums on how to deal with spyware.	*Maybe you can find tracking software in the apps section of the control panel? You could also check your firewall to see if there is anything that you do not recognise being allowed through. However, if there is tracking software installed, then uninstalling it could make him suspicious. Equally, I'm not sure that searching for information about tracking software is a good idea if you suspect he might be tracking you.* [NGOF]
	Blocking and Communication	Describes the ways in which victims manage their communications with perpetrators.	*If you maintain contact, at least keep it strictly to email. It's probably less disruptive than phone calls or texts.* [NGOF]

Table 1. Themes, subthemes, descriptions of subthemes, and illustrative quotes

access, surveillance was achieved by monitoring victims' posts and interactions on social media, or as the quote below demonstrates, through common app features such as read receipts.

> *The man I am dating says that he will beat me if he ever finds me cheating. He says that he is watching me on social media to make sure that I don't fuck him over.* [CF]

> *He knows when I wake up in the morning because he sends me a text at night, after I'm asleep, and when he sees it's been delivered, he knows I'm up. I noticed this because, within 5 minutes of waking up, he's usually at my door.* [CF]

Victims are also expected to always be available through digital technologies, whether it be instant messages (IMs) or phone calls. Victims fear the consequences of not replying immediately or within the timeframe expected by the perpetrator. As one victim describes, not being immediately available to answer perpetrators' IMs and calls led to various forms of threats and abuse.

> *He constantly called me when he was away or I was in another place. If I don't answer the phone, or if I don't answer quick enough, he calls me a whore. He leaves voice messages, texts, and emails that are filled with treats and abuse.* [NGOF]

Even when engaged in professional (e.g., at work), social (e.g., out with friends), or personal activities (e.g., sleeping), victims are expected to be available. In some of these cases, it is clear how the ubiquity of digital technologies allows perpetrators to monitor and control aspects of a victim's life that were not possible before the ubiquity of personal connected devices. As one victim discusses,

> *He keeps me on the phone for hours at night until I fall asleep while he is still talking. He checks all my calls and messages and I'm not allowed to work 15 minutes late because he'll accuse me of cheating. I must also always be available to pick up the phone, even if I'm at work.* [NGOF]

In addition to always being available, victims are often expected to be locatable. Victims are threatened or coerced into sharing their live location data with perpetrators, which is something that would not be possible prior to the ubiquity of smartphones. It, therefore, constitutes a novel, invasive, remote, and real-time form of coercion and control perpetrated through digital technologies.

> *Does anyone else get texts like this from their abuser for no good reason? I literally live on edge and check my phone incessantly because I'm afraid that if I don't answer*

him immediately, he will spin out of control. I hate this. [Post includes a screenshot of a text message asking the victim to send the perpetrator a pin of her location]. [CSF]

COVERT SURVEILLANCE

Covert surveillance was less common in the forum data and interviews. In covert surveillance situations, victims are (initially) not aware of being monitored. Surveillance is achieved through the use of spyware, keyloggers, or legitimate apps such as those used to track children, pets, and lost devices (e.g., Find my Phone). In such scenarios, victims may suspect they are being monitored but have no confirmation and, quite often, no way of proving the surveillance to others. The transcript below shows how victims can be monitored for a long period of time before becoming aware of it.

> *I am looking for people with similar experiences of being monitored through spy apps. My partner installed Zoemob [a family locator app] on my phone. I immediately lost all my privacy. It was the perfect tool to perpetrate abuse. Although these apps are extremely invasive, they do not seem to break any laws in [country removed]. Is there anyone else out there who has been monitored in this way? The app was covertly installed so, for a long time, I did not know I was being monitored.* [CF]

An analysis of the data also showed that victims were unsure about how to identify covert forms of surveillance. The nature of spyware requires victims to possess a certain level of technical knowledge in order to 1) know that spyware exists in the first place, 2) correctly identify spyware, 3) remove or have it removed, and 4) ensure the device is not compromised again. This was clearly observed in forum posts where victims ask each other for advice on how to detect and remove spyware, as well as in the interview with [S01]. The following transcript illustrates a victim's difficulty in identifying spyware, which the police failed to detect, but was found with the help of a colleague from the IT department at her place of employment.

> *Um, it took me a long time, I stopped using my laptop, it took me a long time, um, to finally find someone who might tell me what's going on. So, we took it in, he hooked it up to the business computer that he has, I don't know. They hook it up to a hard drive, I don't know if you've ever seen them do that, so they can't hack into any of their stuff and he had just opened it, looked at it, and he said "ok, there's a program running in the background, why didn't the police find this?" So, he, I had them destroy the computer, I got another computer but I don't know how he's managing to get into everything.* [Imogen]

Even when spyware was not involved, victims did not have the technical knowledge required to effectively assess whether an account has been breached or how it had been breached. The transcript below illustrates the measures that this forum member took to re-secure her accounts, despite not knowing whether there had been breach nor on which account.

> *I have been on my cloud account from his computer so I don't know if he knew my password or if he hacked my Facebook. I've gone on the cloud and changed my emails address and password. I've changed my password on Facebook too and set up the text alerts if someone is trying to log in.* [NGOF]

The difficulty of identifying covert surveillance means that victims may suspect they are being monitored but are unable to identify the potential source of a breach. As seen in the quote above, this leads to situations in which victims are investing significant amounts of time, under distress, in an attempt to secure all of their accounts/devices.

RESTRICTIONS TO DEVICE ACCESS

Victims often reported cases where perpetrators would intentionally break and/or confiscate their devices, with the aim of limiting access to support or contact with people outside of the relationship. The transcript below shows how the perpetrator confiscated the victim's phone immediately after a physical assault.

> *Today it escalated and he physically assaulted me. I'm fine. I've only got a few bruises so it's nothing serious. Straight after he showed regret and cradled me, bathed me, and dressed me. He took my phone away from me for a while. He's also taken my car and his keys to work today, so I'll have to stay home all day. He's broken me. All I can do is sit on the couch. I can't face talking to anyone or going anywhere. I know I need to leave him. I'm trying.* [CSF]

In addition to confiscated devices, victims also report that perpetrators remove SIM cards or break their devices during or after an escalation in abuse. In all of these scenarios, the aim is to restrict victims' ability to access support, including from family, friends, professionals, or anyone outside of the romantic relationship.

> *He made sure I had no contact with anyone who would be able to support me. He used to remove the SIM card from my phone, smash my phone, or throw it out of the window. I cannot remember how many phones I had during that time of my life.* [NGOF]

Given the nature of IPA, where abuse takes place within the privacy of a home, a mobile phone may be victims' only way of reaching support. However, as the transcripts show, perpetrators are well aware of this and effectively take steps to remove victims' access to devices and consequent support. This victim describes how the perpetrator removed all access to outside support, locked her in the house, and physically assaulted her when he discovered that she was planning to leave.

> *When he found out that I was planning to leave him, he broke my mobile phone, disconnected the landline phones, and locked me in the house for four days. He continuously assaulted me over those four days and told me he was going to kill me. He switched off the electricity (during an incredibly hot summer) and did not allow me to drink any water. I honestly thought I was going to die but then I woke up on the last day and he had just disappeared.* [CF]

THREATS, HARASSMENT, AND ABUSE

In addition to surveillance and restricting victims' access to devices, perpetrators also misuse digital technologies for the purposes of carrying-out ongoing threats, abuse, and harassment. The ubiquity of digital technologies effectively extends perpetrators' reach into almost every aspect of victims' lives. This includes when victims and perpetrators are not physically co-located or in scenarios where internet connectivity would not have been as ubiquitous as it is now (e.g., outside or when commuting). As illustrated by the transcript below, victims report that ongoing technology-facilitated abuse has the effect of emotionally wearing them down.

> *The constant barrage of calls and texts sucks the life out of you.* [CF]

What is more, the possibility of receiving real-time threats, at any moment, keeps victims in a constant state of fear and anxiety.

> *I know he is coming here to hurt me. I received several threatening emails from him stating this.* [CSF]

Transcripts also show that persistent harassment extends to victims' friends and family, potentially leading to the destruction of those relationships.

> *He bombarded me with text messages and phone calls at 4 am. He also contacted the girlfriend that I was out with, bombarding her with abusive messages too. This led her to not want to go out and celebrate her birthday with me. He got his way again.* [CF]

Once a relationship is over and perpetrators effectively lose physical access to victims, abuse and harassment via digital means seem to escalate. The quote below illustrates how the perpetrator leverages contact with his daughter to continue to harass and abuse the mother, via Skype and over the phone.

> *Yeah, well he's, my two older girls' dad so he does call on Skype and on the phone still and often he'll still often be quite nasty to me over Skype or the phone.* [Nora]

Later in the interview, S02 elaborates on how distressing this is. She also explains how she asks her daughters to point the phone's camera away from her so that she is not in the image, despite the perpetrator requesting that his daughters show him their mother. Furthermore, after leaving the abusive relationship, victims' social connections may continue to experience abuse and harassment through email, social media, and other forms of digital communications. This has the effect of placing victims in a state of constant worry that the ex-partner may find out current information about them, such as a phone number or home address. The transcript below illustrates how remote long-term harassment, enabled by technology, can lead victims to worry that they will never escape the abuser.

> *I've changed my phone number and moved into a new house, but he won't stop emailing. He messages my friends, people from work, and my family. Everyone has had to block him. I'm so paranoid about him finding me or my new address. Will this ever end?* [NGOF]

Furthermore, perpetrators' use of new accounts or phone numbers to carry out abuse makes it more difficult for victims to *block* perpetrators, avoid their texts, calls, emails, or prove that the abuse is coming from a specific individual.

> *We became friends through playing video games online. Eventually, we began Skyping and talking until one day he told me that he loved me. He would get angry if I wasn't talking to him whenever I wasn't at work or school. When I tried to break-up he would threaten suicide and engage in self-harm. For about a month he's been creating new accounts to harass me on social media, he's made almost 500 new email accounts from which he sends me messages. He's called my phone more than 100 times. He has contacted at least 10 of my friends and family, almost on a daily basis, and keeps threatening to end my life. It has been six months of getting messages from fake accounts that he's made. He stalks me on social media, which I need for my job.* [CSF]

In other cases, perpetrators leveraged digital communications to make attempts to reconnect with victims. Victims discussed how perpetrators attempt to re-enter their lives after a period of separation through social media, IM, and email. The following transcript shows how one victim felt manipulated, over texts, into agreeing to re-enter the relationship and attend marriage counselling.

> *You won't believe what I did. His [perpetrator's] friend called me, on his behalf, asking to rescind the protection order I had obtained. My ex and I have now been texting. At first, they were harmless texts but yesterday after 5 hours of constant texting I agreed to marriage counselling. How did this happen? I sat in disbelief. He didn't even apologise for threatening and scaring us. I'm beating myself up.* [CF]

Often, forum members were aware that this behaviour would repeat itself every time they attempted to end their relationship with the perpetrator.

> *After a breakup, he eventually starts texting me and reels me back in. He will send me long texts about how he loves me, cares for me, and cries when he looks at old pictures of us together.* [CSF]

These forum discussions reflect the delicate nature of intimate partner abuse as a crime where the victim/survivor maintains romantic feelings for the perpetrator. As exemplified by a forum member's post,

> *It's my birthday today. For most of the night and day, I have been checking my phone constantly to see if he texted or emailed me. He hasn't and I am so upset. I'm crying typing this.* [CF]

Furthermore, victims blamed themselves for maintaining contact with abusive ex-partners, especially if contact then led to renewed abuse. The knowledge of only being an IM, email, or call away means that victims are required to exert immense levels of self-control in order to not contact or respond to perpetrators' communications. In the transcript below, one forum member describes craving contact with the perpetrator and how once contact was established, it quite rapidly fell into old patterns of abuse. The victim then blames herself for exchanging IMs with the abusive ex-partner.

> *I craved his contact and he did contact me on Valentine's Day. He was kind and nice for a few texts and then he turned and hurt me again. I should have predicted this. I should have seen it coming.* [CF]

Communication through digital means was also used by perpetrators to convince victims that they had changed. Particularly, the asynchronous nature of IM means that

perpetrators can adjust their behaviour and consider their replies, making it a lot easier to convince victims of their changed ways. Forum members warned each other of the dangers of maintaining contact with former partners. The following transcript shows how this forum member is hopeful that the perpetrator has reformed, based on their interactions over IM and phone calls.

> *I've been talking with my former partner for the last few days over the phone and Facebook Messenger. We had been apart for a year. He is behaving completely differently. He seems to have changed. He seems happier, he's laughing, saying sweet things, and not getting angry. Could it be that he has really changed after this amount of time? I really hope so because I feel happy and in love again.* [CSF]

On the other hand, in situations of shared parental responsibilities, perpetrators do not need to create a line of communication but can exploit obligatory childcare-related contact to continue the abuse. What is more, in cases where victims may be in a custody battle with perpetrators, they report feeling under pressure to reply to perpetrators' abusive communications, out of fear that not replying may be used against them in family court. In the transcript below, a victim is discussing how she feared *blocking* the perpetrator because this may be perceived by the courts as interfering with communication between the perpetrator and their son. This participant only *blocked* the perpetrator once her son was old enough to communicate directly with his father.

> *Um, he had, you know, a couple of iPads and, um, you know, so he was, he was pretty vigilant with sending a lot of texts to all of us all the time. And I was worried about, you know, turning it off because of what that might do in the courts, you know, about custody for our youngest son. So, for a long time, I left that on and would read it, but I got to the point where I just couldn't anymore. I blocked him so that he couldn't contact me anymore.* [Gianna]

What is more, if access to the survivor is limited, perpetrators often attempt to gather information through their children. On the one hand, as parents, perpetrators have legitimate reasons to stay connected with their children via digital technologies. However, perpetrators also use children and their devices as tools to continue to harass, stalk, and abuse victims.

> *I explained to my daughter that her father and I will only be communicating via email from now on. She asked if I had done that today. I said "yes". Then she said she could've guessed that because he's been texting her relentlessly today.* [CF]

Finally, the non-consensual sharing of intimate imagery was also identified within the wider umbrella of ongoing threats, harassment, and abuse. Cases of intimate imagery being distributed online were fewer than those solely involving the threat of sharing. Nonetheless, the threat is enough to control and manipulate victims who fear the consequences of having intimate imagery of themselves distributed on the internet.

> *She asked him if he was going to share their sext pics and he responded with "Bitch what did I tell you about asking me stupid questions?" She pushed back in a calm manner and he went crazy, verbally and over text until she couldn't get out of bed for days.* [CSF]

In addition to sharing intimate imagery without permission, one forum member describes how the perpetrator attempted to extort money from her in exchange for taking the images down.

> *I tried to report the photos my ex used on his BDSM site [removed], without my consent, to the police. Unfortunately, they couldn't help and I felt a bit ridiculous afterward. The photos weren't nude as such so they didn't think there was much they could do. The photos are still online and my ex wants [amount of money removed] to take them down so that he can get more pictures taken.* [CF]

In some cases, intimate imagery is also shared with victims' immediate social network, as illustrated by the transcript below.

> *After we broke up, he retaliated by breaking into my Facebook and sending my nudes to every guy he thought I had fucked or wanted to fuck.* [CSF]

Based on the transcripts, it is unclear whether the imagery was originally captured with or without victims' consent. What is clear is that the threat, or the actual sharing, implicated non-consensual behaviour.

In summary, Theme 1 details the forms of technology-facilitated IPA being discussed on the forums and by interviewed survivors. Forms of abuse include overt surveillance, covert surveillance, physical restrictions to device access, as well as remotely perpetrated threats, harassment, and abuse.

THEME 2: VICTIMS' USE OF TECHNOLOGY

Theme 2 focusses on how victims are using technology within the context of IPA. It includes two subthemes, namely 1) evidence gathering, and 2) victims' use of social media.

EVIDENCE GATHERING

Forum members advised each other to record evidence of physical and digital abuse for legal purposes, such as child custody cases and protection orders. The discussions reveal how victims feel that the responsibility of gathering evidence of the abuse is on them, in order to avoid situations in which it is the victim's version of events versus the perpetrator's. As exemplified by one forum member's advice to another,

> *If you end up in a custody battle with him, it will be your word against his. You will need to prove that he is abusive towards your baby and yourself. Use your phone to record what he is saying when he is being abusive. Also keep the texts, emails, and take pictures of him being abusive.* [CF]

Similarly, in the case of obtaining protection orders, gathering evidence of abuse is seen as essential for proving the abuse to the police. The nature of IPA means that, quite often, the abuse remains hidden until the victim reports it. However, there is a real fear that the police will not take action unless there is a sufficient amount of evidence, beyond victims' statements.

> *If you have evidence of the constant abuse and harassment, the police will issue him with a harassment warning. Keep all the texts, calls, letters, and take photographs of the balloons [delivered to the victim's house]. Create a file of evidence to show to the police.* [NGOF]

In addition to keeping records of digital abuse, victims encouraged one another to record audio/video of the perpetrator being abusive, and take photographs of physical injuries. In the transcript below, S03 is stating that she would advise another victim to record and document all possible evidence of abuse, including seeking healthcare for any injuries to ensure there is a documented trail.

> *Document everything, report everything, go to the doctor's for everything and get out as soon as possible.* [Gianna]

Evidence was also gathered as an aid for victims to remind themselves of the abusive partner's behaviour. Victims discussed dissociative behaviours and lapses in memory in relation to abusive incidents. Some victims felt it was helpful to keep records of the abuse that they could then use to remind themselves of what had happened, as exemplified by the transcript below.

I don't know how long I stayed after he got physical, for the simple reason that my mind started blocking out the physical violence. I was going through my phone recently and found evidence of another incident three or four months earlier. The way I recorded it makes me think that it wasn't the first time. [NGOF]

Similarly, recording abuse was also seen as a form of combatting gaslighting. *Gaslighting* is defined as a set of behaviours carried out with the purpose of manipulating another into feeling that they cannot trust themselves or their own version of events. With recordings, forum members felt they could verify their own version of events against the perpetrator's version, in an attempt to avoid manipulation.

I started recording our arguments because he keeps saying I've said things that I know I didn't. Or that he didn't say things I know he did. He has been out of town this weekend and it gave me time to listen to the recordings. I can't believe how stupid I've been. I am so fed up. [CF]

Irrespective of the reasons for which victims are attempting to gather evidence themselves, this places them at further risk of abuse. If caught, recording evidence can lead to escalations in abusive behaviours either towards victims or their property, as exemplified in the transcript below.

He started threatening me again and I was secretly recording what was happening. But he caught me, he took my phone, went outside and smashed it on the floor. [CF]

What is more, victims are placing themselves at risk in order to gather evidence without knowing whether the recordings are admissible as evidence. The transcripts below show an example of a question being asked about the validity of self-captured evidence, as well as a typical uncertain response to this sort of question.

Yesterday he lost it and was verbally abusive. I managed to record the sound on my phone. I'm wondering if without his consent it would be inadmissible in court as evidence? [NGOF]

I'm still looking into the legality of recording here. I won't use the recordings unless I know I'm legally able to. In the recording, he says he hopes that I'm recording although he didn't actually know I was. I was holding my phone but I recorded the argument on a mini-recorder in my pocket. I don't know if that amounts to consent or not. But I'll find out before using the recording for anything. [CSF]

Finally, even though victims are placing themselves at risk to gather evidence, they describe difficulty in managing and safeguarding the evidence itself. The transcript below

illustrates victims' difficulty in storing digital evidence across time and multiple devices. However, many other transcripts discussed issues related to evidence being deleted during "good" periods in the abusive relationship and then impossible to recover, or even the technical difficulty in gathering adequate screenshots of abusive communications.

> *I took a lot of pictures of, you know, when he would tear up something in the house, you know, and just the destruction that he would do. I took pictures, I haven't done a good job of making sure that those were all saved somewhere, you know, from one old phone to the next old phone. I'd take the picture and think, you know, well things got better for, you know, even a long time, so I wouldn't save those but I wish I had. I'm not sure how I could retrieve those photos now, or if I'll need them. But you know, a way to do that safely. So, the photographs are very important.* [Gianna]

SOCIAL MEDIA

In addition to using digital technologies to gather evidence, victims also used them to follow abusive former partners' lives, namely through social media platforms such as Facebook and Instagram. Victims report checking former partners profiles, looking at their photos, and seeking information about any new romantic partners. This led to a range of often negative reactions and feelings, alongside a sense that checking on former partners' profiles was a compulsion that needed to be managed.

> *I sometimes look up my ex online (Instagram) and for two years I was secretly hoping his new girlfriend would leave him. This week she did. It took time. I also liked the comparison to an addiction [referring to a previous post in the thread], because trauma really does make us go back for more if we let it. Repetition compulsion.* [CSF]

What is more, victims report feelings of re-traumatisation linked to viewing abusive former partners' profiles. As exemplified by the words of a forum member,

> *I cringe every time I look at my ex's Facebook page and I get frustrated with myself for doing it. I have not seen him in almost three years. I look at his FB page and it feels like I just saw him yesterday. It all comes back.* [CF]

The transcript below further exemplifies how victims are aware of the negative emotional impact of viewing ex-partners' social media profiles and mentions *no contact* as necessary to the healing process. *No contact* refers to absolutely no communication with perpetrators, including *blocking* them on social media, and was widely discussed as best practice throughout the forums and by support workers.

> *I often wonder what he is doing and which woman has now assumed the main girlfriend role or in other words the abused domestic and sex slave. I am still terribly curious about who else he was having sex with while he was with me, but only more pain, anger, and sadness lies there. Some days are very hard though, I land up looking at his social media and regretting it. Each day of no contact is truly another day of healing for us survivors.* [NGOF]

In some cases, victims felt that a former abusive partner was using social media to send them particular secret messages, or that perpetrators' posts were intended specifically for them.

> *I sometimes watch his videos on YouTube. He posts instructional videos on playing the guitar. What I see now though is someone who is very calculated and sends "messages" through those videos. He wears a wedding ring now. It sends a message. The background in which he is playing sends a message. I know the "message" my ex sends when he goes on YouTube but I don't fall for it. I also know he is not happy.* [CF]

Posts containing references to former partners' new partners were then either 1) interpreted as being posted for benefit of the victim, or 2) led victims to question whether the abuse had been their own *fault.* The transcript below illustrates this tension quite clearly.

> *I went on social media and decided to look up my abusive ex-boyfriend. Tonight, I found lots of pictures of him, one of him and his wife smiling and looking like a happy couple. Maybe some of his posts are for my benefit? I just have this very tiny voice inside me that says, "maybe it was me, maybe she makes him happy and it was all my fault, all in my head, all my imagination".* [NGOF]

Finally, forum members also used digital technologies to contact perpetrators' new and former partners. This was done in an effort to protect new partners by warning them about the perpetrator's abusive behaviour. In other cases, contact would be made in an effort to understand if the perpetrator had a history of being abusive, with the aim of validating their own experience. Contact was usually established over social media or email.

> *I also got in touch with my ex-boyfriend's wife. He abused her for most of their marriage. It was so nice to have someone else validate my story. I also got a hold of his new girlfriend's e-mail address and I warned her. Initially, she saw all of the abuse towards me and his wife and she left him. Last weekend she married him.* [CSF]

However, and even though survivors reached out in efforts to protect and warn perpetrators' new partners, this initiative was not always well received nor did it have the desired effect.

> *I had many recordings of when we fought, several police reports, and pictures of bruising when he had violently raped me the second time. He has a new partner. They're acting all happy on Facebook: going to church, cooking together, etc. The same things he did with me. I warned her and she laughed at me. But I wasn't going to walk away and let him get away with the damage he has done to me and so many other women.* [CF]

In summary, Theme 2 illustrates the ways in which victims are using digital technologies within the context of IPA. Victims are using technology for 1) gathering evidence of abuse and 2) contacting perpetrators' new or former partners.

THEME 3: PEER-ADVICE AND PROFESSIONAL ADVICE ON DIGITAL PRIVACY AND SECURITY

The third theme focusses on the support and information, exchanged between forum members or given by support workers, regarding digital privacy and security. It is structured according to the three subthemes below, namely 1) covering digital footprints, 2) hacked or hijacked accounts and spyware, and 3) *blocking* and managing communications with perpetrators.

COVERING DIGITAL FOOTPRINTS

As illustrated in the first theme — *Forms of technology-facilitated abuse* — victims often do not have easy access to a device that they are sure is not being monitored. Therefore, forum members advised each other to cover their online tracks through private browsing, clearing history logs, or avoiding the use of devices that perpetrators are aware of altogether.

> *I've set up an email account that I only log into using private browsing: that way the username & password aren't remembered. I save any notes as draft emails. You could also use Evernote [a note taking app] in the same way if you don't already use it for work or for other notes? Just log into Evernote using private browsing, choose a good password and maybe use an email he doesn't know about to sign-up. This will give you a pretty good way of organising notes in case you do decide to use them as evidence or store advice as well as events.* [NGOF]

On the forums, in situations where victims may be unsure whether a device is being monitored, they advised each other to use a computer in a public space, such as a library. Completely avoiding one's own devices was seen as a fail-proof way of ensuring the perpetrator cannot monitor their digital activity in any way.

> *I can't physically help you but I'm always here online if you need support. Just be certain to wipe your internet history and don't use passwords that he knows or can guess. Hopefully, he's not one of those extremely creepy guys that have spyware on your computer. Although just to be safe, I'd use a computer somewhere else.* [CSF]

Regarding professional advice, support workers commonly advise victims to limit their use of social media and purchase a new phone, in order to remove avenues that perpetrators can exploit for abuse.

> *Um, even if they've blocked them, they'll find new accounts to find them, even if they change their name, there are ways of them get[ing], so my advice to clients is always remove social media. I know it's really hard in this day and age, you feel like you're having to give something up. But at least, for the initial sort of few months, I think it's important.* [Arya]

However, as highlighted by SW06, victims do not always have the financial means necessary to purchase new devices. In such cases, victims have no option but to continue using their devices, even though these may have been compromised by spyware or because the perpetrator knows their access codes.

> *I think it [stalking] is definitely easier now, if you just have the password to someone's iCloud than you can just go on and find their phone and who wants to get rid of their phone? Like, especially the clients that we support, like, they don't have enough money to even put themselves up in a hotel or whatever, so they're not 'gonna get rid of their phone, they just don't have the means and finances to just get a new phone.* [Peyton]

HACKED OR HIJACKED ACCOUNTS

In cases where victims suspected that their accounts had been illegitimately accessed by the perpetrator, advice included changing existing passwords or creating entirely new accounts. Advice on how to detect a compromised account involved general actions such as checking whether emails had been opened or moved to the *trash* folder. The issue with this advice is that perpetrators with basic technical knowledge could easily take steps to not be discovered, such as permanently deleting emails or marking them as unread.

If he has hacked in and deleted emails, are they in the "Trash" folder? If it's Hotmail then you can recover recently deleted emails (if he's deleted them from the inbox and trash folders). If you recover emails you've never seen then you know someone's been in your account. I'm not sure about other email services. I agree with the others that a new email might be best. [NGOF]

In other cases, victims were aware that their accounts had been hijacked but could not take any action to prevent it out of risk of further abuse. The transcript below depicts how the perpetrator has found a workaround that allowed him to use 2-factor authentication — a security measure intended to provide added protection — against the victim. In this scenario, the victim cannot change her own passwords without alerting the perpetrator and has been advised to create entirely new accounts.

She cannot change her passwords because the perpetrator has set up her accounts to use his phone for 2-factor authentication. What she needs is a new email and a new bank account that he does not know about. [CSF]

In order to arrange support with victims, support workers will attempt to assess whether a particular form of communication is secure or not. SW01 states that she often advises victims to change email addresses as a form of avoiding surveillance.

So, going back to when it was in a refuge, that same thing is, that I would say to women here [...] Ahh, change email addresses, don't use Facebook, um. [Quinn]

However, as discussed by SW06, her clients change email addresses quite frequently because they believe that their accounts are being monitored by the perpetrator. This effectively renders it difficult for the support worker to check-in on victims' safety and schedule support.

Sometimes it's very very specific which is really difficult because it obviously limits the amount of support you can give that person, um, especially if they can only be contacted by email, um, I tend not to leave voicemail messages unless they've specifically said that it's safe, and email addresses, I find that with a lot of my clients, that they change them all the time 'cause they're just worried about them being hacked. [Peyton]

In this context, it is clear that support services require an improved process for identifying compromised email accounts and supporting victims in re-securing them or arranging for alternative forms of contact. However, an alternative form of contact may not be possible if support organisations are not equipped with knowledge and

resources necessary to re-secure compromised devices, or inform victims how to use their existing devices more safely (e.g., private browsing).

SPYWARE AND LOCATION TRACKING APPS

Regarding spyware, advice on how to remove it generally revolved around formatting a device or performing a *factory reset.* However, and contrary to the transcript below, most posts sharing advice on spyware did not mention that this type of malicious software can also be transferred from one device to another through restoring old backups. The following transcription was the only transcript, in our dataset, that cautioned against transferring content from a compromised device to a new device.

> *Take your child's birth certificate, medical records, and your banking information. Wipe all the computers in the house, set them back to factory, and reformat the hard drives. You must also get a new mobile phone and do not transfer any apps from your old phone onto the new one, just in case he has spyware on there.* [CSF]

Furthermore, advice was not always accurate regarding how spyware can be installed on devices and not all interviewed professionals were aware of spyware. Even those who were aware of spyware expressed the sentiment that they did not possess the training and knowledge necessary to identify whether a victim's device may be compromised. On the forums, and as illustrated in the transcript below, several inaccurate assumptions were made regarding spyware, namely 1) that installing spyware on a device requires high levels of technical expertise, and 2) that spyware/malware cannot be installed remotely.

> *I don't think that is possible: remote tracking is unlikely unless he is a technology genius. Tracking cookies are set up by sites, not by individuals. I would clear your cache if I were you and run Superantispyware [anti-spyware software]. Then I would run Malwarebytes [anti-malware software]. When you have finished, uninstall these because they take up a lot of space. Very often this will alleviate a slow pc. If you do not live with this man, it is very unlikely he can track you except on social media (like Facebook). In which case delete your account there.* [NGOF]

What is more, in cases where spyware is identified, removing it may not always be the best course of action. Removing spyware effectively alerts perpetrators to victims' knowledge of the surveillance and removes an avenue through which abuse can be carried out, which can lead to increased risk for the victim. Similarly, the transcript below also demonstrates how searching online for information about spyware may, in

itself, be risky for victims.

> *I'm not sure, maybe you can find tracking software in the programs/apps part of your control panel? Or can you check your firewall and see if there's anything that you don't recognise being allowed through? If there is tracking software then uninstalling it could make him suspicious, so be careful. Also, I don't think Googling information about tracking software is a good idea if you think he's tracking you.* [NGOF]

In addition to spyware, there are many legitimate apps that can be misused by IPA perpetrators to monitor victims. Examples of such apps are those used to track children, pets, or lost devices. What was found in the data is that victims are generally unclear on the difference between legitimate apps that share users' location data and spyware. This is demonstrated in the transcript below, where the victim describes an app that her daughter and the daughter's boyfriend have for consensually sharing each other's location, as a response to a question about spyware. The transcript goes on to suggest a *factory reset* of the victim's device, which would not necessarily remove a legitimate app such as Find my Friends. The advice exchanged on the forums, regarding these apps, does not necessarily lead to increased security for victims. In fact, the advice could put victims at more risk due to a false sense of security.

> *There are apps that people can download on their phones to know where you are. It isn't difficult to do. My daughter has an app where she and her boyfriend can see each other's location. It is very easy. You should factory reset your phone and change all your passwords. Your phone is probably very compromised at this point.* [CF]

Although some support workers were aware of the capabilities of location tracking on smartphones, none of the interviewed professionals stated that they would know how to advise a victim who is being tracked. In such cases, professionals advise victims to purchase a new device, which may not be financially viable for all victims. Furthermore, as demonstrated in the quote below, technology was perceived to evolve at such a rapid pace that support workers are unable to keep up.

> *It's about, I think it's managing it and not being aware of exactly how much people can track you and can, um, abuse you through the means of technology. Um, for example, I know on certain phones there's a location's history recorder and that's very discrete, people don't necessarily know that it's recording your locations. So, if a perpetrator was to know that, and to be one step ahead, which often people are because technology is always changing, evolving, we can't keep up all the time. They [perpetrators] can then check that location's history which could put someone at greater risk.* [Rylee]

BLOCKING AND MANAGING COMMUNICATION

In cases where victims are required to maintain contact with perpetrators (e.g., shared custody arrangements), forum members advised managing contact through email or another asynchronous mode of communication, as opposed to face-to-face interactions or phone calls. Asynchronous communication was seen as a way of allowing victims to read communications and reply when they felt able to do so, rather than having to respond to the perpetrator in real-time.

> *If you have children together, create an email account for parenting only and delete any emails that don't relate to the children immediately. That way you can look at the emails when you're feeling strong or when somebody is there to help you.* [CF]

Furthermore, managing communications through IM or email also allows victims to keep records of abusive content. As one forum member advises in response to another's distress regarding court-mandated contact with an abusive ex-partner,

> *A few things that may help to give you back some control: start keeping every text, every e-mail, and record his conversations with you. Start gathering evidence or proof of his abuse. Your ex will do anything to hurt you. Try to be brave and keep a record of what he does.* [CF]

Similarly, support workers advise victims to communicate with authorities (e.g., CAFCASS) through email so that there is a record of the communications. In the transcript below, a support worker describes advising victims to email CAFCASS officers so that there is a record of their conversations, should it be needed in family court.

> *Ahhh, I always encourage women, if they're going to be in contact with, like if they're a CAFCASS client for example, I encourage emailing rather than telephone calls, because then she's got a paper trail of evidence, should she need it.* [Sadie]

Finally, when communication with perpetrators is not necessary, victims advised each other to *block* perpetrators on social media, *block* all their shared contacts, and be cautious about who may be able to view their posts. Victims were also advised to change their phone number and screen any calls from numbers that they did not recognise.

> *I would advise them, if they, first of all, their mobile phone, I would advise them to change their mobile phone number, which is very difficult for women because they've got lists of people [contacts] on their mobile phone but that's what I would advise. I'd*

> *advise them to block them from any email, and their Facebook, and anything that's online to block that person if they could.* [Sadie]

Overall, support workers expressed the opinion that more training on technology-facilitated abuse is necessary. Support workers felt that they did not have the digital privacy and security knowledge that is necessary to advise victims, nor had they received any relevant training.

> *I think there, yeah, there's always plans for that and I think regular training, so keeping us updated on how technology and the cyber-world has evolved is just about time, having enough time to put those things in place.* [Rylee]

All the strategies outlined in this theme effectively place the burden on victims to protect themselves from perpetrators' digital abuse and harassment. What is more, they require continuous labour in *blocking* new accounts and phone numbers that perpetrators create to continue abusing victims.

In summary, Theme 3 highlights issues with the digital privacy and security information being shared on forums and the gaps in support workers' knowledge on the subject. The next section presents a discussion of our three main findings in relation to the aims of the *insight gathering* phase of this work.

3.7 DISCUSSION

The purpose of conducting the interviews and analysis of forum data, reported on in this chapter, was to:

1. understand whether the experiences of technology-facilitated IPA being reported by victims engaging in online peer-to-peer support are the same as those reported by existing research with victims engaged with formal support services;
2. understand if the challenges being faced by support workers in the UK are the same as those reported in existing research conducted in the US and Australia;
3. identify the main technology-facilitated IPA issues being discussed by victims and support workers in order to inform the design challenges for the codesign workshops (reported on in Chapter 4).

The findings detailed in Theme 1, revealed that many of the challenges being faced by victims and support workers are similar to those reported on by research with victims

engaged with formal support services, in the US (Dimond, Fiesler and Bruckman, 2011; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017) and Australia (Woodlock, 2016; Harris and Woodlock, 2018). These issues include harassment and abuse via digital communications, location tracking via legitimate apps such as Find my Friends, and spyware (Southworth *et al.,* 2007; Crisafi et al., 2016; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Chatterjee *et al.,* 2018; Harris and Woodlock, 2018). What this study also shows is that the devices used by perpetrators for abuse are the same as those that victims rely on to seek outside support and navigate their daily lives. For example, on the one hand, perpetrators are using social media, IM read receipts, legitimate apps such as Find my Friends or Find my Phone, to monitor and track victims. On the other hand, as seen in Theme 2, victims use these same technologies to gather evidence of abuse, to access support, to warn former abusive partners' new romantic partners, or to contact perpetrators' former partners with the aim of validating their own experiences.

Previous research had not highlighted the importance of social media for victims seeking to warn other potential victims or validate their own experiences. This could be the case because this sort of discussion may be more common between peers on forums but not in face-to-face support with professionals. Nonetheless, the forum data shows that for some victims, being able to reach out on social media to perpetrators' new or former partners is an important component of their own recovery. Either through a sense of needing to caution other potential victims or by validating their own experience of abuse through exchanging experiences with perpetrators' former partners. However, as described in Theme 3, professionals often advise victims to cease or avoid their use of social media. Avoiding social media has the aim of removing an avenue for abuse that perpetrators can exploit. This reveals a tension between support workers' need to safeguard victims and the potential consequences of isolating them further by limiting their engagement with the digital sphere. Theme 3 also highlighted that the advice support workers give regarding digital privacy and security, which is to avoid all non-essential uses of technology, is largely based on a lack of knowledge and training in this area. Interviewed professionals did not feel they had the training that is necessary to support victims experiencing technology-facilitated surveillance. With technology-facilitated harassment, via texts or email, support workers advise victims to change phone numbers, email addresses, or *block* perpetrators, and close their social media accounts. However, regarding forms of overt or covert surveillance, such as spyware or location tracking via legitimate apps, support workers are less able to provide support as they highlight their own lack of knowledge regarding digital

privacy and security. In fact, one support worker mentions that she expects to learn a lot, in this regard, from the young adult victims she is due to begin supporting in the near future. This may, in itself, showcase a generational gap in tech-related knowhow that is not unexpected and is consistent with existing literature (Kesharwani, 2020).

Similarly, this study found that the information exchanged on the forums regarding digital privacy and security is not always correct, which could, in fact, place victims at further risk. An example of this was the advice exchanged between forum members regarding spyware, which generally failed to highlight that restoring a device from a backup, after formatting it, would most likely reinstall the spyware. This can result in a false sense of security where victims think they are no longer being tracked, when, in fact, the perpetrator still has access to the same level of surveillance as before. In such cases, the victim might attempt to return to a sense of normality by, for example, disclosing the abuse to a friend or meeting a new romantic partner, which could potentially trigger an escalation in abuse.

In this context, it becomes apparent that managing digital security is a complex task for which more effective victim-facing guidance is required. What is more, support workers require the training necessary to identify signs of possible covert surveillance, alongside more general digital privacy and security management knowledge (e.g., privacy settings on smartphones and social media). Currently, and as mentioned in the interviews, third-sector support organisations are undertaking efforts to upskill their workers for digital privacy and security regarding social media and location services. Similarly, a growing amount of research has investigated the use of smartphones and social media within abusive relationships (Southworth *et al.,* 2007; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Harris and Woodlock, 2018).

However, in order to avoid a reactive approach to the Internet-of-Things and smart home devices, this research proposes working alongside support workers and survivors in anticipating these near-future threats before they reach ubiquity. Based on the findings from the interviews and forum data, a set of issues or challenges were created for the codesign workshops. The codesign workshops aim to bring survivors and support workers together in leveraging their life-experiences to anticipate the threats posed by smart home devices, within the context of IPA. Anticipating these threats would allow support services to prepare, in advance, the resources necessary to support victims in a proactive manner, rather than the reactive way in which smartphones and social media issues have begun to be tackled.

To that end, a series of *issues,* or design challenges, were created to guide the codesign workshops. The challenges were selected if 1) they seemed likely to be exacerbated by the shared nature of smart home devices, and 2) were issues that victims and support workers were struggling to deal with at the moment. The challenges are the following:

- **Overt Monitoring** refers to surveillance carried-out, by perpetrators, that victims are aware of. Overt monitoring seems likely to be facilitated by technologies such as smart indoor security cameras.

- **Covert Monitoring** refers to surveillance carried-out, by perpetrators, without victims' knowledge, which could be exacerbated by shared smart home device logs and remote access to video and audio feeds.

- **Remote Threats, Abuse, and Harassment** refer to ongoing abusive communications during the relationship and/or once the victim has left. It was hypothesised, in this work, that technologies such as smart home hubs could enable further perpetration of remote threats and harassment.

- ***Revenge Porn* & *Outing*** refers to the act of using intimate imagery, which may or not have been captured consensually, for the non-consensual purpose of sharing those images with people outside of the relationship. In the case of same-sex relationships, intimate imagery can also be used for the purpose of "outing" someone who has not disclosed their sexuality publicly. Again, technologies such as smart indoor security cameras may increase the risks of *revenge porn* and outing for victims.

- **Capturing and Managing Digital Evidence** refers to the capture and storage of digital evidence of the abuse both during and after an abusive relationship. In the case of evidence of abuse, it was hypothesised that smart home devices could be leveraged to record evidence, or, on the other hand, that abuse through such devices may be even more difficult to prove.

- **Managing Digital Privacy & Security** refers to the processes of managing privacy and security settings across different devices, accounts, and platforms. The complexity of managing privacy and security may be significantly exacerbated by smart home devices, not only due to a larger number of devices to manage but also due to a wider range of proprietary platforms.

3.7.1 LIMITATIONS

The sample size for interviews with support workers was limited to a small number. Nonetheless, nine support workers were interviewed from a range of third-sector support organisations, including those supporting female victims, LGBTQ+ victims, as well as those supporting victims and working with perpetrators on violence prevention programs. In this sense, interviewed professionals offered a wide-range of perspectives on the issue of technology-facilitated abuse. Furthermore, due to the fact that only two of the four survivors were based in the UK, this data was analysed in conjunction with the forum data rather than as a dataset of its own. In this context, the interviews with support workers provide insight into the current support landscape in the UK, while interviews with survivors and forum data provide insight into a much wider range of first-hand experiences of technology-facilitated IPA.

3.8 CONCLUSION & NEXT STEPS

The *insight gathering* study expanded upon existing research conducted in the US and Australia with 1) UK support workers' perspectives and 2) experiences of victims engaged in online peer-to-peer support rather than formal support services.

Overall, the study found that the forms of abuse being discussed on the forums are largely similar to those reported in recent research (Southworth *et al.,* 2007; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Chatterjee *et al.,* 2018; Harris and Woodlock, 2018). However, an analysis of the forum data also revealed that advice regarding digital privacy and security, exchanged on forums, tends to not be accurate or complete, which may place victims at further risk. It also found that UK-based support workers do not feel equipped to deal with the challenges posed by technology-facilitated IPA. In fact, all interviewed professionals agreed that training in this field is required, as none of them had, to date, received any training on technology-facilitated IPA. In both cases, it seems that victims who are engaging in peer-support and those involved with professional support are not currently accessing adequate information and advice regarding technology-facilitated abuse.

In the context of this work, it was hypothesised that the nature of smart home devices may exacerbate technology-facilitated IPA. The shared nature of smart home devices affords less interpersonal privacy between household members than personal devices, such as tablets and smartphones, or analogue devices, such as door locks and

thermostats. Access to remote video feeds of the house through smart indoor security cameras, access to smart door lock and thermostat device logs, and remote control of devices such as smart home hubs are, for example, a few features that reduce users' interpersonal privacy within the same household. They reduce interpersonal privacy because they provide information such as when a user entered or left the house or what activities the user is currently engaged in. With the aim of adopting a proactive approach to support provision, this work aims to engage support workers and survivors in envisioning the threats posed by the near-future ubiquity of smart home devices. The next chapter describes a series of codesign workshops that involved survivors and support workers in using creative methods to predict the near-future consequences of smart homes on IPA.

The interviews and forum data allowed for the identification of six *issues* that were used to inform the codesign workshops described in the next chapter. Each of these issues was selected, based on an analysis of the data and on the finding that 1) current advice on how to tackle them is not readily available, and 2) they are susceptible to being exacerbated by the domestic and shared nature of smart home devices. Accordingly, the next chapter expands upon the codesign workshops' procedure, participants, methods of analysis, and main findings.

4

IMPLEMENTING: CODESIGN WORKSHOPS

Findings from the interviews and forum data (see Chapter 3), as well as existing research (Southworth *et al.,* 2007; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Chatterjee *et al.,* 2018; Harris and Woodlock, 2018), show that digital technologies are being leveraged by perpetrators to intimidate, threaten, monitor, harass, or otherwise abuse victims of intimate partner abuse (IPA). The main technologies that victims report being misused are social media, online accounts (e.g., email), and location services on, for example, smartphones and fitness trackers. Findings also show that survivors and professionals do not, currently, have the knowledge necessary to effectively manage their digital privacy and safeguard themselves from perpetrators (Southworth *et al.,* 2007; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Snook, Chayn and SafeLives, 2017; Harris and Woodlock, 2018).

Furthermore, recent reports have found that smart home devices are increasingly being used as tools for IPA. Although statistics are not yet available for these emerging threats, in 2019 alone, Refuge reported almost 1,000 cases of IPA involving devices such as smart home hubs and smart TVs (Elks, 2018). 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 adopted in this work brings survivors and support workers' experiences of technology-enabled IPA into better understanding the challenges that near-future smart home devices pose to victims. The hypothesis, on which this work is based, is that issues will be mainly related to the shared nature of smart home devices, along with shared access to remote feeds and usage logs, as well as differing levels of permissions for users in the same household.

Accordingly, the aims of the codesign workshops with survivors and support workers are to:

- understand participants' main concerns regarding surveillance and abuse in the context of near-future smart homes;
- engage participants in co-creating solutions to support victims of surveillance and abuse enabled by smart homes.

4.8.1 CHAPTER STRUCTURE

This chapter details the codesign workshops with survivors and support workers. It includes a description of the workshop procedure, along with participant characteristics, the ethical considerations that informed the workshop design, and the qualitative data analysis methods that were used.

After the workshop methods and procedure have been introduced, the main findings are presented. Findings are structured according to five themes:

- Theme 1: How intimate surveillance and abuse enabled by smart home devices starts
- Theme 2: How intimate surveillance and abuse is perpetrated on a daily basis
- Theme 3: The current response to intimate surveillance and abuse
- Theme 4: Underlying issues
- Theme 5: Participants' ideas for addressing surveillance and abuse enabled by smart home devices

A brief discussion of the findings is then presented and followed by a conclusion and the next steps that lead in Chapter 5.

4.1 WORKSHOP PROCEDURE

Each codesign workshop lasted 2-2.5 hours and was structured as follows:

- Presentation of research findings to date
- Video: Smart Homes
- Collaborative activity: Narrative creation
- Video: Speculative Product Demo
- Collaborative activity: Mapping data misuse
- Break
- Collaborative activity: Ideation

The interview and forum data analysis findings, discussed in Chapter 3, were presented at the beginning of the workshop. This was done with the aim of contextualising the research and framing the issues that would be addressed in the collaborative activities.

The first video illustrated what a smart home is while contextualising technologies such as indoor cameras and remotely controlled door locks. 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 feeds of indoor video footage. This was achieved through an aesthetic common to technology promo videos (Fig. 8), by using clips from existing product advertisements, in an effort to highlight technological capabilities in a visual language that is characteristic of new tech products. The video was intended to provoke thinking rather than imposing any particular view on participants.

Following the first 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 supplied with an A3 sheet that included a persona, prompt questions, and a layout for creating scenarios. These scenarios were intended to be speculative and set the scene for the ideation activity. Most participants were not familiar with smart devices nor the Internet-of-Things (IoT). In fact, some participants did not know whether their phones were smartphones or not. Therefore, the video, through which an understanding of smart devices and data was built up, was fundamental to the success of the workshops.

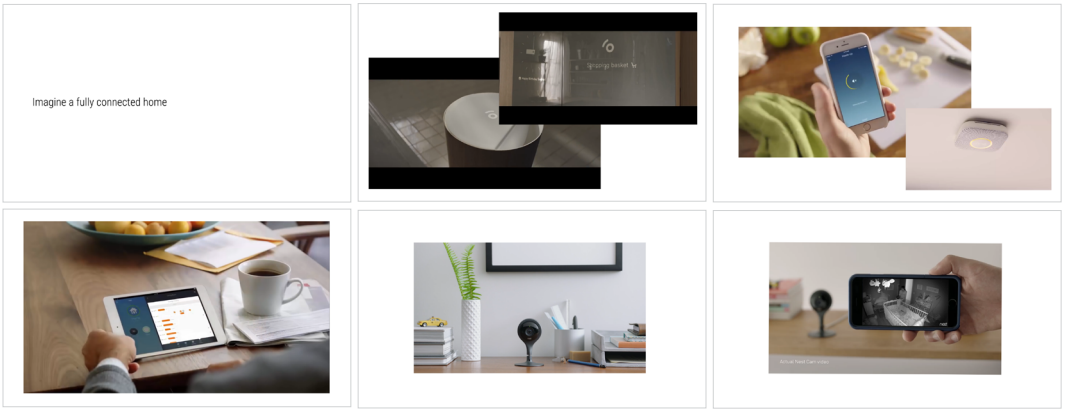

Fig. 8. Screenshots of smart homes video

A second video was then used to set the scene for the data mapping activity. In the data mapping activity, participants were prompted to consider a range of devices and the types of data they collect, how that data could be misused by perpetrators, and what support victims would need. The video took the form of a short product demo,

again following an aesthetic aligned with common technology promos (Fig. 9). 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, share health and fitness data, as well as follow one another's social interactions. Although dystopian in nature, the video employed a techno-optimistic and uplifting visual language, with the aim of presenting itself as a marketable product, rather an explicit critique. The data mapping activity sought to encourage participants to consider how devices and data can be exploited by an abusive partner.

For the final *ideation* activity, a series of prompts, in the form of A5 cards (Fig. 10), 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. The issues on the cards are based on the findings from Chapter 3. Once a goal and an issue had been selected, participants could combine "smart devices" and "interaction/behaviour" cards to support idea generation.

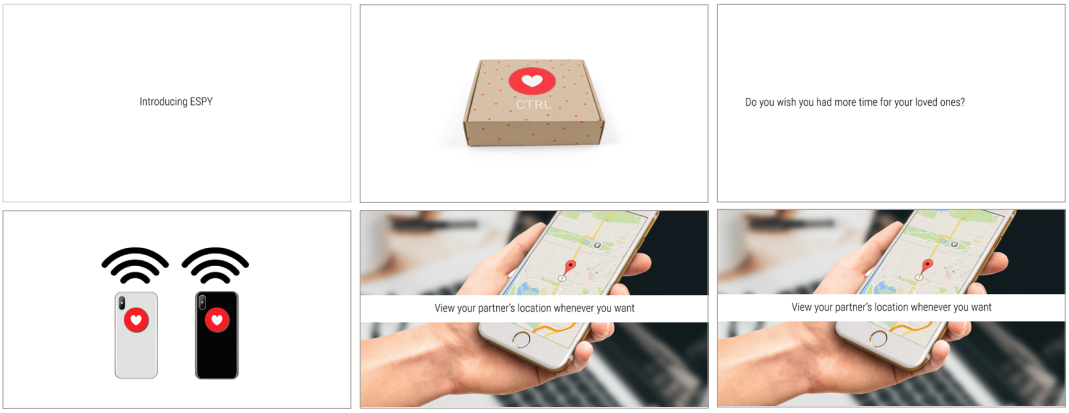

Fig. 9. Screenshots of speculative product video

Speculative materials such as videos have been widely used within design research to support scenario building and ideation alongside workshop participants (Vines et al., 2012; Blythe et al., 2016; Elsden et al., 2017). The videos used in this PhD's workshops served two main functions: 1) equipping participants with the background knowledge on abstract concepts such as smart homes and surveillance, as well as 2) scenario-building and setting the scene within a near-future context of pervasive intrapersonal surveillance. Speculative practices within design have also been explored, in a similar way to this PhD work, as a tool for anticipating cyber-security threats (Faily, Parkin and Lyle, 2012;

Merrill, 2020) and collaboratively designing out opportunities for crime and its impact (Gamman and Thorpe, 2011). As stated by Dunne and Raby in their book Speculative Everything: Design, Fiction, and Social Dreaming, "[by speculating more] we can help set in place today factors that will increase the probability of more desirable futures happening. And equally, factors that may lead to undesirable futures can be spotted early on and addressed or at least limited" (2013, p. 6).

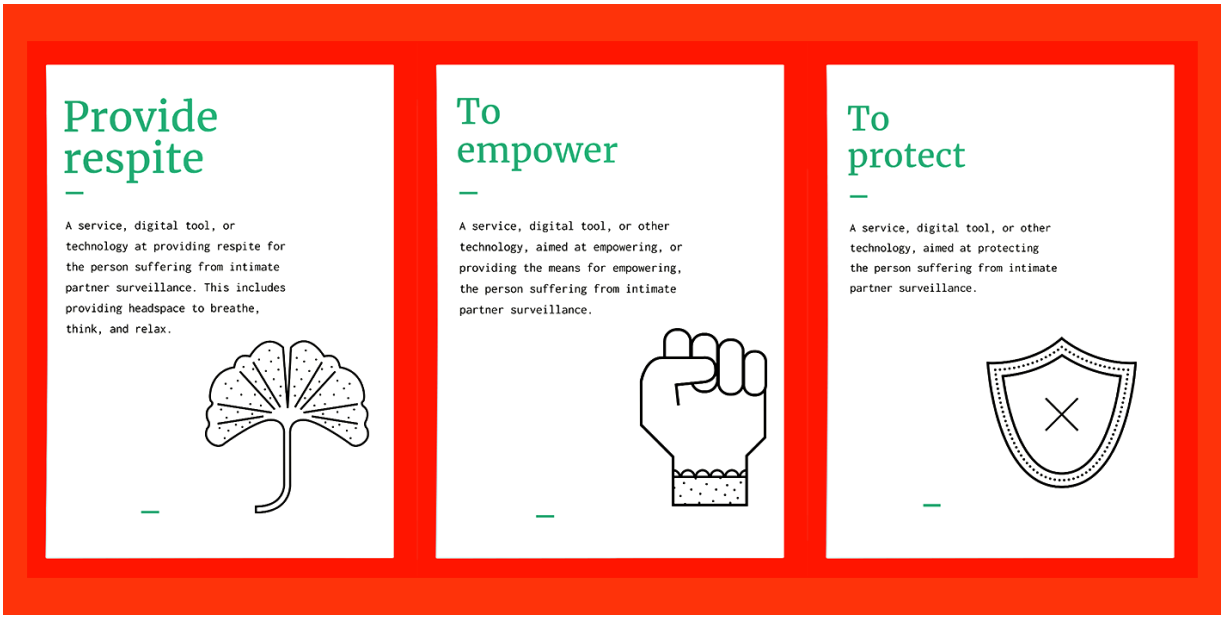

Fig. 10. Examples of the cards used in the ideation activity

The workshops were wrapped up with time for discussion and feedback, giving participants the opportunity to express their thoughts and expectations, as well as provide feedback.

4.1.1 WORKSHOP PARTICIPANTS

The first workshop [W1] took place in July 2018 in the East of Greater London, with 7 survivors [S] and 2 support workers [SW]. All participant names have been replaced with pseudonyms. Participants divided themselves into two smaller groups [G] in order to collaborate during the workshop activities. Participants were regular attendees at a local support group and allowed me, as a researcher, to intervene in one of their meetings by conducting a 2.5-hour speculative workshop with them.

Nine support workers, from two charities, participated in the second [W2] and third workshops [W3], both held in London. One in July and another in September 2018.

Participants in the second workshop worked exclusively with victims, while those in the third workshop had experience of working with both victims and perpetrators.

The fourth workshop [W4] was run with 28 support workers in Yorkshire, England, in October 2018. Professionals were divided into 5 smaller groups for the collaborative activities. Some of the participants worked with victims and perpetrators.

A further two workshops took place in collaboration with a charity based in the Southeast of England in March 2019, one with survivors [W5] and another with professionals [W6]. Six survivors and two support workers took place in the morning workshop, while 12 professionals participated in the afternoon workshop. Two groups were formed in the morning workshop and four groups in the afternoon one.

4.1.2 ETHICS

All participants were sent a copy of the Participant Information Sheet (Appendix C) and Consent Form (Appendix D) at least one week in advance of the workshop. Participants received these materials from the lead contact at each of the charities, rather than from me, in order to avoid compromising potential participants' anonymity, whilst allowing them to express any concerns and/or ask questions about the study with someone not directly involved in it. I did not have any contact with participants who are survivors prior to the workshops.

Participant Information Sheets informed participants that the intention was to video record during the workshops, solely for the purposes of data analysis. However, at the beginning of the first workshop, a survivor became distressed by the camera and asked that the session not be recorded. The decision was then made to not record video in any of the workshops, using instead audio recordings, in order to avoid causing discomfort to any further participants.

In each of the survivor workshops, at least one support worker was present. Support workers were asked to attend the survivor workshops in case anyone required additional support as a result of participation. Workshop activities were structured around *personas* who are survivors of IPA, with the intention of focussing participants' attention on the *persona,* rather than asking them to recall specific accounts of their own experiences of abuse. Furthermore, the near-future focus of the workshops allowed participants to create scenarios that were based on their lived experience of IPA but did not require the direct re-telling of their experience. The workshops placed

participants in a space of creativity and storytelling, rather than in the narrations of their own traumatic experiences.

4.1.3 WORKSHOP ANALYSIS

Workshops were transcribed for analysis, alongside the written materials completed by participants (Fig. 11) during the collaborative activities. A thematic analysis (Saldana, 2015) was conducted on the workshop transcripts and written materials related to accounts of 1) the ways in which perpetrators misuse smart home technologies for IPA, 2) victims and support workers' strategies for tackling IPA enabled by smart home devices, as well as 3) participants' ideas for addressing IPA enabled by smart home devices. 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 (Fig. 13).

An initial phase of descriptive, process, and *in vivo* coding was carried-out based on a first reading of the transcripts. 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 in the next section.

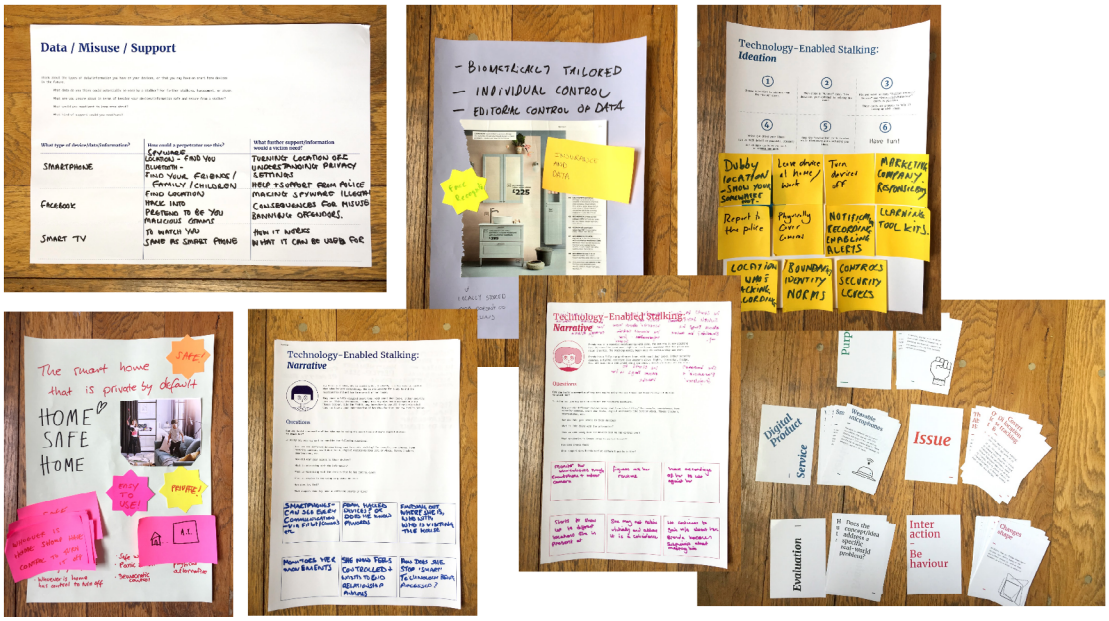

Fig. 11. Workshop materials

4.2 WORKSHOP FINDINGS

Workshop findings are reported on in this section according to five themes. The first three themes, respectively, describe how 1) intimate surveillance and abuse, through smart home devices, begins and 2) how it is perpetrated on a daily basis, as well as 3) participants' strategies to cope with it.

Fig. 12. Images from codesign workshops (taken with participants' consent)

The fourth theme discusses two broader issues underlying technology-enabled IPA. Namely, participants' confidence in their own digital privacy knowledge, as well as the preparedness of support services and authorities to deal with these novel challenges.

Finally, the fifth theme details participants' ideas for addressing IPA enabled by smart home devices. Ideas fell into two broad categories 1) digital privacy training and education resources, and 2) smart device affordances and features.

Each of these five themes is expanded on in the next sections, alongside illustrative transcripts from the workshops.

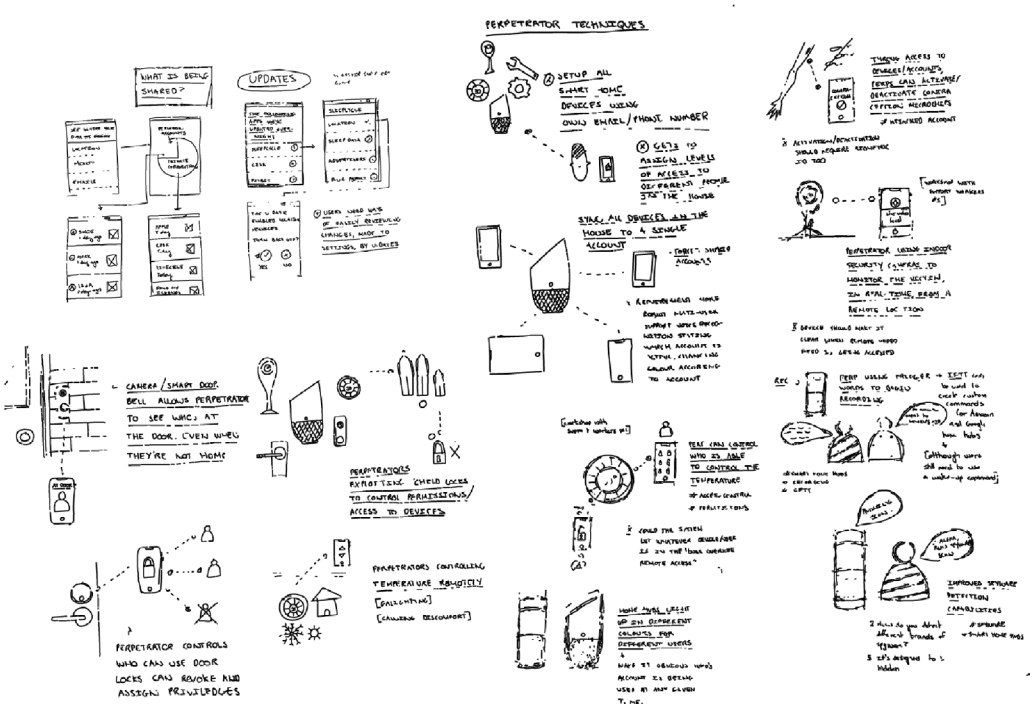

Fig. 13. Sketches of participant idea generation

THEME 1: HOW INTIMATE SURVEILLANCE AND ABUSE ENABLED BY SMART HOME DEVICES STARTS

During the scenario creation exercise (see Section 4.2), participants were prompted to think about how a perpetrator may gain access to, or put in place, the devices necessary to carry-out intimate surveillance. Accordingly, this first theme explores scenarios created by participants that describe how intimate surveillance can be initially established within an intimate relationship.

Firstly, participants described several scenarios in which perpetrators coerce victims into allowing themselves to be monitored. Quite often this was depicted as happening subtly, at the beginning of the relationship, under the guises of 1) perpetrators' concern for victims' safety and 2) leveraging expectations of mutual trust within an intimate relationship. For example, perpetrators will express concern over a victim's safety to justify installing indoor security cameras or a smart doorbell on the victim's property. As discussed by participants, this serves the dual purpose of creating the illusion that the perpetrator is preoccupied with the victim's wellbeing, while (temporarily) masking the underlying motivation of enabling surveillance.

[Sofia-W5-G2-S3] *It might be that he was saying that he just wanted her to be safe, that's quite frequent, isn't it?*

[Zahra-W5-G2-S1] *Yeah, pretending that he cares and that he's just trying to protect her [in order to install cameras].*

In many of these scenarios, perpetrators set up the newly bought devices and ensure that victims either do not have their own account or have an account with fewer permissions than that of the perpetrator. The transcript illustrates this scenario unfolding with smart indoor security cameras.

[Brett-W2-SW] *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. Are they living together?*

[Erin-W2-SW;Adrian-W2-SW] *Yeah.*

[Adrian-W2-SW] *So everything was probably set up on his email, his phone number.*

[Brett-W2-SW] *And on, just the application is downloaded to his phone only.*

[Adrian-W2-SW] *Possibly. No, you know how they have like a main service or a main account and then they have like a secondary account? He could possibly be the administrator account.*

Limiting victims' permissions and access has present consequences by limiting freedom through ongoing surveillance, but also future consequences. In the latter case, if victims manage to successfully end the abusive relationship, they may still be left with devices that they do not have the necessary permission to effectively use or re-secure. What is more, victims may unwittingly be using devices that the perpetrator still has access to. The consequences are that victims may experience a false sense of security where they may feel safer because the perpetrator is no longer physically present, but do not realise they may still be under remote surveillance.

Regarding participants' second point — leveraging trust in intimate relationships to instil surveillance and abuse — victims may willingly share login credentials because they believe they are in a mutually trusting relationship. Existing research with victims of IPA shows that this is often the case (Southworth *et al.,* 2007; Matthews *et al.,* 2017; Freed *et al.,* 2018). Unsurprisingly then, participants expressed the opinion that sharing passwords is common in the early stages of abusive relationships.

[Daisy-W1-G2-S] *Of course he will. 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.*

Furthermore, if victims are not forthcoming with login details out of their own accord, perpetrators may coerce victims into sharing their credentials by leveraging social norms and expectations of mutual trust within intimate relationships. The quote below describes how a perpetrator coerces a victim into sharing passwords by associating unwillingness to share with having something to hide.

[Taylor-W4-G4-SW] *You know as well, "if you don't give me your password, you must be having an affair".*

[Emily-W4-G4-SW] *Absolutely, yeah.*

[Taylor-W4-G4-SW] *Yeah, all that crap.*

Another transcript illustrates how the same goal can equally be achieved in a less confrontational manner. The same transcript also shows how this sort of coercion can make it harder for the victim to immediately realise that what is happening is part of a larger abusive pattern, whilst also removing opportunities for declining the perpetrator's request without causing conflict.

[Masha-W4-G4-SW] *But you can do it really romantically, can't you? You know, "the password is you and me babe" 'cause you're not going to want to change that, are you?*

[Emily-W4-G4-SW] *You [the perpetrator] can do that "we've got nothing to hide from each other".*

Participants discussed the fact that further along in a relationship, or once it is over, perpetrators would have a lot of information about the victim. This knowledge could enable them to guess passwords and/or answers to security questions. In the transcript below, participants are discussing re-securing smart door locks once a relationship is over. Participants are concerned that the perpetrator may gain access to the system password by guessing the victim's answers to common security questions such as *"what is your mother's maiden name?"*

[Andy-W4-G1-SW] *But then depending if that's an online system, could he then hack into it? 'Cause it depends if the device has changed, or, I don't know how they [smart door locks] work ...*

[Matilda-W4-G1-SW] *Normally they have like a control centre type thing …*

[Andy-W4-G1-SW] *That's what I thought, you know, like your WiFi. You change your WiFi password but if he's aware of her secret questions, could he then hack that further? And is it a case of having a manual lock put back on?*

Participants also disclosed many insecure password practices during the workshops. Participants discussed using easily guessable combinations, such as birthdates, or even writing passwords down in notebooks. In cases where perpetrators are familiar with victims' habits and routines, guessing such passwords or finding notebooks, may not be a challenge.

[Sara-W4-G3-SW] *And people often use the same password for the same thing as well, so …*

[Ayana-W4-G3-SW] *…yeah, I do …*

[Sara-W4-G3-SW] *… I do too.*

[Darcey-W4-G3-SW] *It could be a case of snooping through handbags and purses for passwords …*

[Nantia-W4-G3-SW; Sara-W4-G3-SW] *Yeah.*

[Sara-W4-G3-SW] *People write their passwords down, don't they?*

[Group] *Yeah, yeah.*

Even for systems involving the security of one's home, such as smart door locks, participants described having passwords based on birthdates or other memorable personal information.

[Fatima-W5-G1-S2] *Yeah, but you could do that with a CCTV and you could do that on your phone and you wouldn't have to have a door lock. If you use, most people if they have a door lock they're gonna use a birthdate or something he would already know [as a password].*

In summary, this first themes exposes three main avenues that perpetrators can exploit to gain access to, or install, the devices necessary to carry out surveillance and abuse:

1. coercing victims into allowing devices that enable surveillance to be installed in their homes;
2. coercing victims into sharing login credentials;

3 gaining information about victims that facilitates the hijacking of their devices and accounts.

The next theme characterises participants' views on how smart home devices can be used to perpetrate intimate surveillance and abuse on a day-to-day basis, once the perpetrator has access to, or has installed, the necessary devices.

THEME 2: HOW INTIMATE SURVEILLANCE AND ABUSE IS PERPETRATED ON A DAILY BASIS

Many queries and concerns surrounding the functioning of home devices, such as the Amazon Alexa or Nest Thermostat, emerged in the workshops. Participants were unclear as to how user permissions within a household are managed by smart devices on a daily usage basis. Accordingly, the discussion mainly centred on 1) device logs that include all household members' usage history, 2) remote control of devices, and 3) remote access to live video and audio feeds. Given the complexity of this theme and for the purpose of clarity, each subtheme is presented individually below.

HISTORIC SMART HOME DEVICE USAGE LOGS

In the case of historic device logs, participants were concerned that data relating to all household members would be available to the perpetrator in a centralised aggregated log. For example, any search query made to a digital assistant (e.g., Amazon Alexa) would be accessible to the owner of the account used to set up the device. This was found to be particularly problematic in cases where the user is performing queries, which the perpetrator is then monitoring.

> [Emily-W4-G4-SW] *What I wanted to ask is, can you interrogate Alexa to find out what someone else's preferences have been? What someone else has been asking for? What someone else is …*
>
> [Isabelle-W4-G4-SW] *… yes …*
>
> [Taylor-W4-G4-SW] *… yes, of course, it has a history, it's a computer …*
>
> [Sam-W4-G4-SW] *… and there's an app …*
>
> [Emily-W4-G4-SW] *… he [perpetrator] would most probably interrogate it [the usage log] if that's the case …*

In the case of home hubs, door locks, thermostats, and other home appliances, participants were concerned that the historic logs indirectly provide information about when a user is in the home. For example, door lock logs will show who has entered or exited the house and at what time, or a smart thermostat might turn on to regulate the temperature when a user is in the house. A perpetrator with access to these logs would be able to infer when the victim is at home, or not, without the victim realising that device data is being misused for this purpose.

> [Sayeeda-W4-G3-SW] *There's a lot of potential as well with the smart door locks to set times when she might be out at work or college or whatever so it can enable his own access to kind of do a bit of …*
>
> [Darcey-W4-G3-SW] *He can even use them to check at what time she left …*
>
> [Group] *Yeah, yes.*
>
> [Sayeeda-W4-G3-SW] *So what time she comes back …*
>
> [Ayana-W4-G3-SW] *Yeah, yeah, I think that's probably it.*
>
> [Sayeeda-W4-G3-SW] *To get in?*
>
> [Sara-W4-G3-SW] *It's a technology freehouse around these things, absolutely. I would imagine there's a facility on there to check what time somebody has left [the house] …*

Being able to monitor who comes into the home can also be a powerful way of limiting victims' disclosure of abuse to friends and family. If perpetrators know who victims are with, this may be a powerful deterrent for victims to not disclose out of fear of the consequences to themselves and to the recipient of the disclosure, thus, compounding victims' isolation from potential sources of support.

> [Blake-W4-G5-SW] *He'll know when she's in and when she's out and where she goes. So, I'm guessing to being with he'd be monitoring her …*
>
> [Stacey-W4-G5-SW] *… what time she comes in and out and stuff like that … […]*
>
> [Robyn-W4-G5-SW] *And then who comes and goes …*
>
> [Blake-W4-G5-SW] *… oh, yeah, yeah, like friends and …*
>
> [Robyn-W4-G5-SW] *… yes, yes, anyone who comes and goes …*

Furthermore, historic logs can be used to confront victims about their daily activities

and any discrepancy between what they say they did compared to what the perpetrator observed by piecing together information from logs.

> [Emily-W4-G4-SW] *[…] I'm assuming, with the technology with the smart doorlocks, you'll be able to access and see who came or that someone came in at a particular time and left at a particular time …*
>
> [group] *…yeah …*
>
> [Emily-W4-G4-SW] *…so, if you're then questioning someone and saying "so, what were you doing today? Oh, I was wherever. Well, then how come at 11:29 someone left the house and at 11-whatever someone came back in?" So, there must be, they must have the technology for that. Technology to track movements.*

On a daily basis, this effectively allows very little manoeuvre room for victims to access support, as any alteration in daily routine can be monitored and questioned by the perpetrator.

REMOTE CONTROL OF SMART HOME DEVICES

Regarding remote control of smart home devices, participants described situations in which perpetrators leveraged devices to remotely harass, perturb, and cause distress to victims. Regarding smart home hubs, participants' examples included perpetrators remotely playing songs, setting unwanted reminders, and sending audio messages to the victim in the home.

> [Matilda-W4-G1-SW] *You can set Alexa basically to do anything. So you could set 'Alexa, set a reminder …'*
>
> [Ezra-W4-G1-SW] *… You scare mum for 3 am, start blasting …*
>
> [Dani-W4-G1-SW] *Play songs at anti-social hours.*
>
> [Andy-W4-G1-SW] *Yeah, so could be waking her up, she could have lack of sleep.*
>
> [Matilda-W4-G1-SW] *But you could leave a message that says "I'm gonna kill you".*
>
> [Andy-W4-G1-SW] *"I'm watching you". Yeah … "I'm gonna kill you" and prove it. Prove that message came through Alexa at that time.*

In some cases, even when the relationship has terminated, remote access can be leveraged to contact the victim, provided the perpetrator still has access to the device

in question. Based on participants' experience, it would be likely that the perpetrator owned the main account used to set up the device and would, therefore, be the only user with permissions to add/remove users (see Theme 1). The transcript below illustrates the case of a perpetrator sending audio messages, through a home hub, to the victim after a separation.

> [Andy-W4-G1-SW] *… You can leave reminders for people …*
>
> [Matilda-W4-G1-SW] *… You can leave messages, so you can say 'Alexa set a reminder for …'*
>
> [Andy-W4-G1-SW] *… 12 o'clock 'I love you. I miss you. Come back.'*

For smart home appliances, participants described scenarios in which perpetrators would deliberately disturb the basic functioning of the house. Several reasons, or end goals, for creating such disturbances were outlined by participants, which included gaslighting, control, physical discomfort, fear, and intimidation. Switching lights on and off was often discussed as an effective way to instil fear, as seen in the following transcript.

> [Mariam-W1-G2-SW] *[…] So, digital lights, obviously [perpetrator could] turn the lights on and off, yeah?*
>
> [Dana-W1-G2-S] *That's going to spook you, isn't it?*
>
> [Aailyah-W4-G4-SW] *With the smart lights when you gave that example of when you were in the bath …*
>
> [Sam-W4-G4-SW] *…yeah, you could turn them on and off …*
>
> [Aailyah-W4-G4-SW] *… you could terrify a victim, couldn't you? Imagine if you're in the bath all alone or whatever.*
>
> [Sam-W4-G4-SW] *… yeah, my brother tortures me with them. I'll be at Sam's house and I'll know he [brother] will be home so I'll just be turning the lights on and off [laughs].*

In addition to using smart home appliances to create fear, participants also expressed worry that such devices could be misused to gaslight. Gaslighting is a form of coercion and control and refers to the process of manipulating someone into doubting their own memory, perception, and sanity (Abramson, 2014). In the following transcript, survivors discuss the use of a smart thermostat as a weapon for perpetrating gaslighting.

> [Mariam-W1-G2-SW] *You could turn the heating up or down, couldn't you, with one of them?*
>
> [Dana-W1-G2-S] *It could make you feel like you're losing your mind.*

Participants also detailed scenarios in which perpetrators subtly alter the functioning of devices in the home to make victims think that devices are malfunctioning. In the next transcript, participants discuss how a perpetrator manipulates a smart door lock to make it seem as if it is "glitching". This conversation also illustrates how it would be difficult for the victim to identify whether the device is being manipulated by the perpetrator, or whether it is indeed malfunctioning. Furthermore, it highlights how this form of abuse can be extremely difficult to prove to friends and family.

> [Brett-W2-SW] *Amy doesn't know what's happening with her because if Adam [the perpetrator persona] is controlling her in a way like closing the door when she wants to go out like three times and a fourth time he will let her out, she can't be sure that he's doing it or it's her mind playing with her.*
>
> [Amira-W2-SW] *Or if it's the technology. How quick are we to blame technology for stuff not working?*
>
> [Adrian-W2-SW] *"Oh, there's a fault in there" or "the systems not working".*
>
> [Erin-W2-SW] *Well, you can hear it right now, can't you? You can just hear the person saying "Oh, you know ..."*
>
> [Amira-W2-SW] *"... it glitches".*
>
> [Erin-W2-SW] *Yeah.*
>
> [Brett-W2-SW] *yeah, and if she asks her friends to come and check, it's you know Adam can see it's a friend so I will open the door. No one can ever really see [the odd behaviour].*

Another fundamental component in *gaslighting* was the disparity in technology-related knowledge between perpetrators and victims, as described by workshop participants. Participants felt that perpetrators often had more knowledge than victims, which was explained by gender differences related to culture and upbringing, where an interest in technology is fostered in young boys but not in girls.

> [Brett-W2-SW] *And also the stereotypical view that men are more on technology and devices. And because of the gender upbringing, so we still raising our daughters to play with dolls while the boys can play with the computer. So, I think they [boys] are more educated and because they are doing more DV [domestic violence] so, it's the whole situation is just [unbalanced] ...*

This leads to scenarios in which victims rely on the perpetrator to fix devices that are

perceived to be malfunctioning, rather than investigating the issue themselves. Thereby reinforcing the cycle of *gaslighting* by keeping the real issue hidden from the victim and promoting reliance on the perpetrator.

> [Ayana-W4-G3-SW] *She's probably really confused. She's gonna feel quite worn down, isn't she? If things are kind of constantly appearing to go wrong [devices appearing to malfunction].*
>
> [Sayeeda-W4-G3-SW] *Yeah.*
>
> [Sara-W4-G3-SW] *And she won't actually know she's being monitored, will she? She won't know what's going on, you know … [unintelligible]*
>
> [Ayana-W4-G3-SW] *Over-reliant on Mark [the perpetrator persona] and over-dependent on Mark.*
>
> [Group] *Hmmmm.*
>
> [Sayeeda-W4-G3-SW] *Yeah, because he's coming in to save the day ["fix" the devices].*

Furthermore, remote control over home appliances can be used to create physical discomfort for the user in the home. The transcript below illustrates how a smart thermostat can be used to remotely make the house too hot or too cold for the victim.

> [Sayeeda-W4-G3-SW] *I think using the heating as well, um, you know if she's at home and he's switching the heating round and you know, her being uncomfortably cold. Umm, switching hot water off if she's got to mess with the washing machine settings if she's got an important, then so she's not got the things she's expecting to have.*
>
> [Nantia-W4-G3-SW] *Yeah, yeah.*
>
> [Darcey-W4-G3-SW] *It's like interfering with your lifestyle, isn't it?*
>
> [Sayeeda-W4-G3-SW] *Yeah, just the routine.*
>
> [Sara-W4-G3-SW] *Just general interference, yeah, true.*

In fact, two support workers, in different workshops, had experienced cases where perpetrators were harassing victims by remotely changing the temperature in the house.

> [Leah-W5-G1-S1] *It was a very complex case. [A]nd then there was one particular weekend where I was in contact with her and she was "I'm so cold. I'm so cold." so I said "turn the heating up" and she said "every time it up, he turns it down — the husband".*

SMART DEVICE REMOTE LIVE STREAMS

Live audio and video feeds that can be accessed remotely were also extensively examined in the workshops. Devices such as indoor security cameras and smart doorbells enable users to access remote live videos and audio of the inside the home or whenever someone rings the doorbell. Users can access these feeds on their smartphones, at any time and from anywhere. If another user is in the house, the remote user can see and hear what they're doing, provided they are within range of the cameras and microphones. Depending on how many cameras are in the home, participants were preoccupied that almost every aspect of a victim's life could be monitored in real-time.

> [Zahra-W5-G2-S1] *Checking what she's doing every minute of the day and how she's spending her time.*
>
> [Sofia-W5-G2-S3] *Can you record what is happening as well?*
>
> [Zahra-W5-G2-S1] *I think so [...]*

Surveillance can either be accomplished overtly — when victims are aware of the surveillance — or covertly — when victims are not aware of being monitored. In the transcript below, participants describe a scenario in which the perpetrator is monitoring and overtly interrogating the victim based on what is being observed through the live feed.

> [Ezra-W4-G1-SW] *So when we used to go on holiday, obviously these two [points to participants in the group]. These two would stop in the house and housesit and I used to be able to watch ... there were no cameras inside, and I'd be able to see the dogs sat there waiting to go out. But you can imagine, had it been a perpetrator, "where are you going?"*
>
> [Andy-W4-G1-SW] *"You're not going out wearing that"*
>
> [Ezra-W4-G1-SW] *"Why is your car not on the drive[way]?"*
>
> [Andy-W4-G1-SW] *"Why you got make-up on like that?*
>
> [Matilda-W4-G1-SW] *"Who's that man that's just knocked on the door?"*
>
> [Andy-W4-G1-SW] *"Saw you eye the postman up."*
>
> [Group] *Yeah.*

[Dani-W4-G1-SW] *"Where were you until 11 o'clock last night?"*

[Ezra-W4-G1-SW] *And you can text them what they're doing in that moment, right? "I can see you" …*

[Dani-W4-G1-SW] *So, if he's got remote access, then it's …*

[Andy-W4-G1-SW] *That's dangerous, isn't it?*

In the case of covert monitoring, participants discussed whether spyware could be installed on smart home devices to enable covert remote recording/streaming of video and audio, without the victim being aware of being recorded. This could be used, for example, to enable smart home hubs to stream audio from inside the home to a device of the perpetrator's choosing. Given the shared nature home devices, participants thought it would be easier for a perpetrator to install spyware than it would be, for example, on the victim's personal smartphone.

[Mariam-W1-G2-SW] *And that would be the same for all of them* [devices]*, wouldn't it? Him living there. So, I'm wondering if, you know you get spyware now* [for smart home devices]*? Which you can* [now] *download onto someone's phone, do you know about that?*

[Daisy-W1-G2-S; Maria-W1-G2-S] *No.*

Remote feeds were also a concern with smart doorbells, where a user is notified via their phone whenever someone rings the doorbell or motion is detected by the front door. Unlike the smart door lock logs, with the doorbell perpetrators are notified in real-time about who is at the door and can even access a live video and audio feed from the doorbell camera and microphone.

[Zahra-W5-G2-S1] *If there's cameras* [on the doorbell] *he can check can't he — all the visitors?*

[Julia-W5-G2-S2] *Yeah, who's coming …*

[Zahra-W5-G2-S1] *… who's away from the house.*

Depending on the number of cameras in the home, victims can experience difficulty in getting support from friends and family, or even outside the house given that perpetrators can monitor whether victims are at home or not, as well as for how long. Furthermore, realising an escape plan or packing an emergency bag (Women's Aid, 2015; IDAS, 2019) can be difficult if victims know they might be being watched at any given time.

[Emily-W4-G4-SW] *Remote surveillance. And that app that is supposed to be there to help you — like if someone knocks at the door to deliver a parcel you can communicate and do that … well, that's just another way, yeah, but it's actually remote surveillance …*

[Sam-W4-G4-SW] *… yeah but then he can see other people who are going into the house …*

[Emily-W4-G4-SW] *… yeah, see who comes in and out.*

[Isabelle-W4-G4-SW] *If she wanted to go and someone came to help her [the perpetrator could see through the cameras] …*

[Emily-W4-G4-SW] *… can you imagine if you were planning on leaving?*

[Isabelle-W4-G4-SW] *Yeah, and he'd saw the bags gettin' packed …*

[Taylor-W4-G4-SW] *… yeah, all those things that you do discretely while no one is watching …*

[Aailyah-W4-G4-SW] *… yeah, even the support worker coming for a visit if she didn't know that camera was there …*

The capture of non-consensual intimate imagery was also widely discussed in the workshops. Participants feared that perpetrators would misuse devices such as indoor security cameras to capture images that could then be used as leverage to threaten and control the victim. In the following transcript, participants discuss the use of intimate imagery to threaten and coerce a victim.

[Sara-W4-G3-SW] *And if you connect this to indoor cameras as well, yeah, there's gonna be times that she's gonna be getting changed. So what's the gonna do with that evidence?*

[Sayeeda-W4-G3-SW] *Well, yeah, he could use that as …*

[Darcey-W4-G3-SW] *… he could take a recording of her and blackmail her …*

[Sayeeda-W4-G3-SW] *… yeah, create stills …*

One group even discussed the capture of intimate imagery post-separation, where the perpetrator would be able to witness if the survivor had a new intimate partner. Of course, in such cases, the perpetrator would need to still have access to the device without the survivor knowing. Existing research on IPA shows that abuse often continues for many years after separation, which could render such a scenario more likely than one would initially expect.

[Aurelie-W4-G5-SW] *Yeah but then he can also use those [intimate photos]. They're leverage, aren't they?*

[Aisha-W4-G5-SW] *They could be used to blackmail …*

[Group] *Yeah, yeah …*

[Stacey-W4-G5-SW] *And particularly if she starts seeing other people.*

Another form of abuse enabled by remote feeds, that was discussed in the workshops, was control over what victims eat. This form of control is common in abusive relationships *"[t]he perpetrator supervises what the victim eats, when she sleeps, when she goes to the toilet, what she wears. When the victim is deprived of food, sleep, or exercise, this control results in physical debilitation. But even when the victim's basic physical needs are adequately met, this assault on bodily autonomy shames and demoralizes her"* (Herman, 2015). With cameras inside a smart fridge, participants examine how victims' food intake is susceptible to being remotely monitored by perpetrators.

[Leah-W5-G1-S1] *They can check what you're eating [smart fridge card] 'cause that's another way of abusing, isn't it? To withhold food …*

[Maryam-W5-G1-S3] *Does it tell you what's in the fridge?*

[Fatima-W5-G1-S2] *Yeah, we all use it through Tesco. If you go to your own Tesco or whatever it does an online shop. So if you say "I've run out of milk" it will reorder milk. It's just so easy.*

[Leah-W5-G1-S1] *I've heard more than one woman say that food is a way they're controlled.*

[Maryam-W5-G1-S3] *Yeah, food, yeah.*

[Leah-W5-G1-S1] *So, you couldn't covertly sneak into your fridge and get something 'cause they'd know …*

Monitoring food consumption was also related to belittling and body shaming, which is common in abusive relationships and has the effect of fostering victims' dependency on perpetrators by lowering their self-esteem (Herman, 2015). The following transcript illustrates how perpetrators use food consumption to belittle victims,

[Emily-W4-G4-SW] *I've just been thinking as well, we've been talking about smart fridges and you've got cameras within to see inside the fridge and so if someone is remotely accessing that and you've got a guy who is, um, part of his controlling behaviour is*

"what are you doing eating that? You're supposed to be losing weight". That's just going to be horrendous, isn't it? "I know exactly what you've taken from the fridge, you know, at what time and you've ..." and that's just another [form of control]. Horrendous.

It is important to note that many of the scenarios described by survivors do not require the perpetrators carry-out surveillance 24/7. The fact that victims know they could be watched, at any given moment, leads to a *"panopticon effect"* (Foucault, 1977). This effect means that victims will behave as if they are being watched because they do not know when they are not being watched. For this reason, victims police their own behaviour to match what they think is expected by the perpetrator, leading to constant states of alert, self-monitoring, and fear. In the transcript below, a survivor describes how she feared using her phone, several years after separation, because she did not know if the perpetrator was still able to monitor her.

[Zahra-W5-G2-S1] *I didn't even use a phone in the end because he was telling me that he could listen to all my calls. And that was for the landline as well. And I'm still like that 3 years later, thinking, you know, people are listening to me and all that. Awful.*

[Researcher] *And then I guess you don't even know how much of it is true and how much isn't but because he's told you that he can listen to your mobile phone and your landline, and you have no way of ...*

[Zahra-W5-G2-S1] *... I mean, I got a new mobile phone but then he was saying "well, I can do it without you, without going near your phone".*

In summary, during the workshops, participants discussed three main ways through which intimate surveillance and abuse could be perpetrated, on a daily basis, using smart home devices:

1. access to shared historic device usage logs;
2. remote real-time control of home devices;
3. remote real-time access to live video and audio feeds.

While Themes 1 and 2 detailed how intimate surveillance and abuse is initiated and perpetrated on a daily basis within the context of smart homes, the next theme describes participants' strategies to address these issues.

THEME 3: THE CURRENT RESPONSE TO INTIMATE SURVEILLANCE AND ABUSE

The third theme, that emerged from an analysis of the data, focusses on participants' strategies for coping with intimate surveillance. The theme includes survivors' self-reported strategies, as well as advice given by professionals as stated by professionals themselves. The two subthemes are *non-use* and *managing digital privacy. Non-use* refers to participants' views that opting-out of using any new technologies is the most effective form of avoiding intimate surveillance. *Managing digital privacy* shows participants' strategies for managing their own devices and data when use is perceived to be essential. Each of these is expanded upon, in turn, below.

NON-USE

When prompted to discuss what kind of support a victim suffering from intimate surveillance would need, participants mainly discussed removing all smart devices from the home. In all workshops, participants expressed a lack of confidence in their ability to effectively manage their digital privacy. Not owning or using any smart devices was overwhelmingly seen as the only way for victims to be certain that they are not being monitored. The transcript below illustrates how professionals find it necessary to either remove victims from their homes — the place where the smart devices are, or destroy all the devices if victims remain in their homes.

> [Aurelie-W4-G5-SW] *If she then like, taking at some point that she works it out that it's through her home system, what does she do then? Does she move? Does she go stay in a hotel? Does she have relatives she can stay with?*
>
> [Charlie-W4-G5-SW] *Well, she may get rid of everything.*
>
> [Aurelie-W4-G5-SW] *Does she burn everything? Does she sell everything?*
>
> [Blake-W4-G5-SW] *Disconnect, yeah …*
>
> [Aurelie-W4-G5-SW] *Does she go round the house with a sledgehammer when she's had enough?*

Survivors expressed the same sentiment, describing how the solution may be to disable all smart devices in the home.

[Alex-W4-G2-SW] *Yeah, yeah, we did. Technology isn't always the answer, at least not in this case.*

[Edith-W4-G2-SW] *She could disable all the devices that he has access to, which is not really stopping it [capture of intimate imagery] …*

A particular concern with non-use takes place when a smart device has replaced an essential appliance or mechanism. Examples are door locks, thermostats, or doorbells. If victims do not trust that the smart device is secure, they may need to replace it. This would, of course, place a significant financial burden on the victim, who may still be recovering from financial abuse. In the transcript below, participants discussed how one route may be to replace smart devices with manual/analogue ones, as a form of being able to trust that they are safer.

[Dani-W4-G1-SW] *Then what would she do in response? So she would have to change her locks … there's a lot of things that the poor victim has to do!*

[Ezra-W4-G1-SW] *Yeah.*

Participants were already using strategies of non-use to protect themselves and their children. Often, even long after an abusive relationship is over, victims still do not trust digital technologies. Although not directly concerning smart home devices, in the ensuing transcript, a survivor describes turning off her children's phones when they return from spending time with the perpetrator.

[Maya-W1-G1-S] *I don't have any of these things [smart home devices]. I refuse to use these things. I haven't got a clue. Apart from my iPhone, I don't use, I mean the kids have got iPads, most of the time I turn them off. I mean, he bought my son a mobile phone and as soon as he walks in the door from his dad's it's [the mobile phone] off.*

[Eva-W1-G1-SW] *So you know you can do that locate my phone?*

[Maya-W1-G1-S] *Yeah, I turn it off every time [names removed] comes home.*

[Eva-W1-G1-SW] *That's a good idea.*

What is more, professionals are advising victims to either not bring their smartphones with them to appointments or to not enter information into their digital calendars.

[Maryam-W5-G1-S3] *Something I will say about this as well, when I see clients, I tell them to never put it in their phone — when they're coming to see me.*

[Leah-W5-G1-S1] *Yeah, yeah.*

[Maryam-W5-G1-S3] *And they look at me really strange. Just write it down.*

[Fatima-W5-G1-S2] *It's just like with doctors' appointments, put it down in a card. Never on the phone. None of it is on my phone.*

However, non-use was also seen as a way of further isolating the victim, meaning that it was seen as a less-than-ideal solution. The following transcript illustrates the concern that opting-out of using digital technologies will have the effect of isolating victims and, therefore, placing them at greater risk of further abuse.

[Amira-W2-SW] *It's gonna end up with that thing like you see in movies where you've got the old guy who's off the grid and doesn't touch technology and unless they sort these problems out, it's gonna force people away from technology not towards it.*

[Erin-W2-SW] *And isolate people more, which could essentially create more abusive situations. 'Cause yes, this is very scary and it's creating a massive situation where you could be abused but then if you then become really scared of all of this [smart homes] and take yourself away from all of that, then you're even more, potentially, even more vulnerable.*

Furthermore, the transcript below reveals the tension where a support worker is arguing that not using technology is not a longterm solution that promotes survivor empowerment, while a survivor is arguing that she would rather be safe than use such devices.

[Maya-W1-G1-S] *Removing batteries.*

[Anna-W1-G1-S] *Putting all the devices in a sort of locked place.*

[Eva-W1-G1-SW] *Changing passwords.*

[Anna-W1-G1-S] *The way we think in the end is don't have the devices in the first place.*

[Eva-W1-G1-SW] *Yeah, that's not a long term solution though, is it? Because life is moving forward no matter what and we're in the world we're in.*

[Anna-W1-G1-S] *Yeah, but we're so used to having to change our ways and not have anything. Like, I'd rather, if it was happening to me now, I'd rather have like a little brick phone [laughs]. And I know it's not …*

Non-use was also interpreted as a less effective tactic for the younger generations. Participants expressed the feeling that younger victims may not be willing to limit their usage of novel technologies, as this could come with significant social trade-offs.

> [Masha-W4-G4-SW] *See that's interesting because my reaction is "buy a shit phone and drop the phone that you think you're being tracked with, in the bath. But then I'm thinking, "if I said that to the kids, they'd just go 'fuck off', actually" …*
>
> [Emily-W4-G4-SW] *… yeah but the point that was made there about they've got so much of the rest of their life invested in the same device …*
>
> [Masha-W4-G4-SW] *… and it's so isolating to be cut off. Yes.*

Furthermore, *non-use* may not be a viable option if the victim is still in an abusive relationship. As shown by the quote below, victims may place themselves at further risk if they opt for non-use, therefore, alerting the perpetrator that they are aware of and counteracting the surveillance.

> [Brett-W2-SW] *The main problem with all this is if you snooze it [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 …*
>
> [Erin-W2-SW] *… but you could find your opportunity, couldn't you? So you could wait until they'd left the room or something. Or …*
>
> [Adrian-W2-SW] *… but wouldn't it show on the log, like "snoozed at 5:45 pm"?*
>
> [Erin-W2-SW] *Yeah, but they wouldn't know at the time. So at the time, at least that isn't being recorded. And if a, not always, but if they are doing this then they're probably not actively doing it, you know, they're probably not telling the person that they're doing this. So how could they then come to them and say "oh, by the way, when we were having this conversation you snoozed it, don't do that again". 'Cause that then sort of defeats the object.*
>
> [Adrian-W2-SW] *Yeah, [defeats] what they're doing. Mmmmm. Unless they're like openly controlling.*

Finally, a few participants also questioned why victims/survivors should be required to give up technology to protect themselves, arguing that all that would be necessary would be improved privacy management.

[Masha-W4-G4-SW] *I think the thing about it is it is the same with technology, which is when we think back to all that stuff about the "good" advice that we give, which is switch it all off. Because my first reaction is "get rid of the smartphone. Get a basic phone that takes phone calls". Actually, your whole freaking life stops at that point. So, I couldn't get here, I can't get home, I have no hotel booking without my smartphone. I have no idea who any of my friends are. Everything gets switched off if I get rid of my smartphone now.*

[Sam-W4-G4-SW] *And it's like why should they …*

[Masha-W4-G4-SW] *… why should I? Yes.*

[Aailyah-W4-G4-SW] *You've just got to make sure your privacy settings are spot on.*

This effectively places the onus on victims/survivors to protect themselves, either through non-use or through the meticulous management of privacy settings. The latter leads to the next subtheme, which discusses participants' approaches to managing digital privacy.

PARTICIPANTS' STRATEGIES FOR MANAGING DIGITAL PRIVACY

Overall, managing digital privacy was less discussed in the workshops than non-use. Non-use was participants' preferred strategy for preventing intimate surveillance. However, when non-use was not a viable solution, other strategies were discussed. The main strategy was that of changing passwords.

[Maya-W1-G1-S] *Yeah. "What strategies is Diana using to protect herself?"*

[Anna-W1-G1-S] *Um, this is the hard one, isn't it?*

[Eva-W1-G1-SW] *So what strategies you'd use sounds pretty good …*

[Anna-W1-G1-S] *Just turn it off …*

[Eva-W1-G1-SW] *… you change your passwords.*

However, if, for example, a smart device has been set up with the perpetrator's email address and password, the victim may not have the necessary permissions to re-secure the device. In the transcript below, participants talk about how the perpetrator may be the only one with full permissions to control a smart thermostat.

[Erin-W2-SW] *But if he's the one setting everything up then he's the one that if something was to go wrong, he'd have the passwords and things, so if they needed, if she later*

on down the line realises what he's doing, she might not have the access to be able to stop him. 'Cause they — whoever the company is that she might call out, it would say but you're not the main person on the account or you don't have the password.

Another strategy was to reset or "factory restore" devices, which involves the erasing of all data on a device and then setting up new device accounts.

[Sara-W4-G3-SW] *I mean she needs to like reset everything. [laughs]. I don't know what to say!*

However, once again, the main user's account details may be necessary to perform a complete reset of the device. Furthermore, participants also expressed the feeling that victims are under high levels of stress during and after separation from the abuser, whilst managing several devices and accounts can be overwhelming.

[Maya-W1-G1-S] *What kind of support would a victim need for emails? Umm, need to change them. I had to change all mine.*

[Anna-W1-G1-S] *Yeah, I do anyway.*

[Eva-W1-G1-SW] *And was it an easy process?*

[Maya-W1-G1-S] *No, it's a hard process …*

[Anna-W1-G1-S] *It's really hard.*

[Maya-W1-G1-S] *… yeah, especially when you're stressed.*

[Anna-W1-G1-S] *And then you've got to remember them because you don't want to write them down in case someone finds …*

In summary, participants discussed strategies to deal with smart home surveillance and abuse that are based on their current experiences of abuse enabled by smartphones and social media. Participants' strategies focussed on non-use as a form of removing possible avenues of abuse, as well as managing privacy through changing passwords and resetting devices. However, the former may come at a significant financial burden, while the latter relies on victims having the necessary system permissions, which may not always be realistic. The next theme contextualises the issues underpinning Themes 1-3.

THEME 4: UNDERLYING ISSUES

This theme focusses on the topics underlying participants' concerns about smart home devices and their preference for *non-use* as a self-protection strategy. The underlying

topics have been identified as 1) a general gap in knowledge regarding data capture & storage, data sharing, and privacy management, as well as 2) the understanding that support services are ill-equipped to deal with these novel challenges.

PARTICIPANTS' TECHNOLOGY AND DIGITAL PRIVACY MANAGEMENT KNOWLEDGE

As demonstrated in the previous themes, participants did not feel that they fully understand the capabilities and limitations of smart home devices, to an extent that would allow them to safeguard themselves from surveillance and abuse. For example, it was assumed that if a smart door lock was installed, that there would be no manual backup, thereby allowing for scenarios where the perpetrator could lock a victim in the house remotely.

> [Julia-W5-G2-S2] *With the smart locks …*
>
> [Sofia-W5-G2-S3] *… locking somebody in.*
>
> [Zahra-W5-G2-S1] *Yeah, absolutely.*

The same was observed with smart appliances, as participants created scenarios in which perpetrators remotely locked the fridge or turned off the gas supply to the stove. Although it may be possible to turn a smart stove hob off remotely, a user in the house can still turn it back on and smart fridges do not generally include locks.

> [Adrian-W2-SW] *Or controlling the gas so that she can't cook anything.*
>
> [Erin-W2-SW] *Yeah.*

Participants also discussed whether remote control could be achieved from any distance or whether the user was required to be within a certain range of the device, even though some participants owned devices such as the Amazon Echo.

> [Alex-W4-G2-SW] *Ok. But if he didn't want to give the game away, he could just monitor her?*
>
> [Edith-W4-G2-SW] *He could be really creepy and just make noises through Alexa. He could change songs. He could play their favourite top 5 romantic songs. He could be quite mindful …*
>
> [Alex-W4-G2-SW] *You can do that off-site? Just anywhere in the world?*
>
> [Edith-W4-G2-SW] *I'm not sure how far, but I know if your phone's connected and you're connected to that Alexa, you can then … I only know from experience of making some funny shopping lists on my partner's Alexa.*

Furthermore, participants expressed that they do not know how initial access to home appliances is granted In the first place. Participants wondered whether these devices require a password or whether proximity to the device and a WiFi password, are sufficient to connect a user's smartphone to the device.

> [Edith-W4-G2-SW] *And I'm not sure whether those devices have passwords, do they? 'Cause Alexa is Wifi, if somebody comes into your house and connects to your wifi, they can connect to Alexa. Yeah, as far as I'm aware, there is no ... […]*
>
> [Charlotte-W4-G2-SW] *Right, OK.*
>
> [Edith-W4-G2-SW] *You can just pick, your phone picks up what's around, doesn't it?*
>
> [Freya-W4-G2-SW] *But you'd still need, like for our [smart] camera even if you came into our house and you connected yourself to the WiFi, you couldn't access the camera without the password and account. But I don't know if that's the same for Alexa.*
>
> [Edith-W4-G2-SW] *Yeah, I just Alexa I know is just WiFi and then you pick up the Alexa.*
>
> [Charlotte-W4-G2-SW] *And you can access it even without a password?*
>
> [Edith-W4-G2-SW] *You can control it from your phone and if you've got the Alexa app and Amazon whatever ...*

In addition to issues around permissions and access, participants also expressed difficulty in understanding what type of data is collected by each device, where it is stored, and who it is available to. Throughout the workshops, participants asked each other questions about where data goes when it is stored on the cloud and how it can then be accessed.

> [Zahra-W5-G2-S1] *Ahhh, cloud storage, I don't understand much about that technology.*
>
> [Julia-W5-G2-S2] *Umm, cloud storage is so, everything I've got in my phone is also stored in the cloud somewhere [laughs]. So, even if I delete it off my phone, it would still all be somewhere in the cloud.*

The complexity of understanding where data is stored and who has access to it meant that participants were uncertain of their ability to manage their digital privacy. One group discussed a possible false sense of security associated with managing privacy settings where users have the impression that they've secured their data, when in fact, they may have failed to completely delete or restrict access to it across devices.

[Erin-W2-SW] *I feel like I would need more information on how to like cleanse your data. Because I would be really paranoid that I've said "oh yeah, clear this, clear that" but there might be something that I've missed that you don't even think about. Like, for example, the cloud, be like "oh, you've taken it off your phone, it's gone, done" but no, it isn't. It's still somewhere …*

Compounding these concerns were app updates and hard-to-use privacy settings. Participants debated the number of devices and individual applications that need to be individually checked and adjusted according to individual user's privacy needs, agreeing that the complexities of managing all of them are beyond what they feel capable of effectively coping with. Furthermore, participants expressed the fear that even if they did adjust all their privacy settings, these might be erased or changed without warning when the software is updated.

[Maria-W1-G2-S] *Problem with that is when you update your things [devices] it [privacy settings] goes back to basic, so you have to turn everything off again.*

For participants, the main goal in managing privacy settings was not to protect their data from third-party corporations, but rather to safeguard their data from another user of the same shared device — interpersonal privacy. Overall, participants felt that gaps in knowledge related to smart home device' functionality and privacy management place them at a significant disadvantage in safeguarding themselves against intimate surveillance and abuse. This was equally true for survivors and support workers, which leads to the next subtheme exploring participants' confidence in effective support regarding technology-enabled abuse.

SUPPORT SERVICE PREPAREDNESS AND BELIEVABILITY

In the workshops, support workers were aware of the fact that current service provision and risk assessment procedures are not equipped to deal with technology-facilitated IPA. Currently, support services are struggling to upskill their workforce with the knowledge necessary to tackle abuse facilitated by technologies such as social media and location services. It is unsurprising then that participants felt equally unprepared to support victims in cases where smart homes devices are being misused for abuse.

[Erin-W2-SW] *Yeah, there does need to be more awareness and I think that should start with the support workers. I think if we're gonna be honest, we don't have that much training on this. We don't have …*

[Adrian-W2-SW] *… we'd need a longer degree for this …*

[Erin-W2-SW] *… it should be, it should be a cyber training course. We don't have a cybercrime/stalk, um, course.*

[Amira-W2-SW] *[unintelligible]*

[Erin-W2-SW] *I don't think they have any real mention of it anywhere in our training.*

[Brett-W2-SW] *Only revenge porn maybe.*

In the UK, it is common for support workers to use a standardised risk assessment form — the DASH — to measure the level of risk that a victim may be in. The result of this risk assessment is then used to create safety and support plans with the victim. However, the DASH does not yet include questions related to technology-facilitated abuse. Such issues may be uncovered through discussing other questions on the form, such as *"Does (.....) constantly text, call, contact, follow, stalk or harass you?"* (Richards, 2016) but this can depend on many factors. These factors include the professionals' experience in using the form, in asking follow-up questions, or whether the victim is aware of being monitored, meaning that intimate surveillance can go unnoticed and unaddressed by existing risk assessment procedures.

[Amira-W2-SW] *And then this [technology-facilitated abuse] needs to be on the DASH.*

[Adrian-W2-SW] *Oh, ok, yeah.*

[…]

[Amira-W2-SW] *But what I'm saying is I think — you know we were talking about the pregnancy question in the DASH [Domestic Abuse, Stalking, Harassment and Honour based violence Assessment Tool]? Ahh, [name removed]? They need to update it to have cyber questions.*

[Erin-W2-SW] *Yeah, they do.*

[Adrian-W2-SW] *Yeah.*

Furthermore, professionals highlighted the feeling that perpetrators often seem to be "omnipresent", where they know information that seems unlikely that they would have access to regarding the victim. Professionals often suspected this is achieved through digital surveillance, but their training and risk assessment procedures do not equip them to better identify what the source of information/data may be.

[Julia-W5-G2-S2] *I remember I used to work in a refuge and a lot of women would say "I don't know how he's found me" or "I don't know how he's got this information" but even as a support worker, I don't know the answers because I don't know about technology. A lot of us don't, really.*

Professionals even questioned whether a victim of technology-facilitated abuse would be believed by support professionals, especially regarding novel technologies such as smart home appliances.

[Amira-W2-SW] *I mean I think the key thing there is about believability. I think we, you know, as an organisation as a whole, we need to be gradually moving more and more into the thing of actually going "well, oh, this stuff does happen". It can happen. We need to take this claim seriously until it's proven that actually, it's not quite what we think it is.*

Furthermore, participants' concern that support services were not equipped to deal with technology-facilitated abuse extended beyond third-sector organisations, to law enforcement and health professionals. Participants felt that authorities may not understand, or even believe, victims when abuse is being perpetrated through technology. The transcript below illustrates the concern that not only do authorities lack the knowledge to adequately support victims, but also that victims' mental health might be questioned when reporting technology-enabled IPA.

[Maria-W1-G2-S] *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.*

[Dana-W1-G2-S] [chuckles]

[Mariam-W1-G2-SW] *No, they don't take it seriously, do they?*

[?] *No.*

[Maria-W1-G2-S] *Even when it's criminal, they don't, they don't do anything.*

[Julia-W5-G2-S2] *So we could say get expert advice. I mean, who even has that? I wouldn't know where to go!*

[Ava-W5-G2-S4] *There are tech companies that would do that but chances are they'll think you're nuts anyway and that you're just being stupid and paranoid.*

Compounding all of this was the sense that technology moves too quickly for support services to keep up, even if training was to be put in place. In the following transcript, support workers express the sentiment that it is unfeasible to match the pace of technological development.

> [Erin-W2-SW] *But … I just think it's, there's so much to it.*
>
> [Brett-W2-SW] *Mmmm [yes].*
>
> [Erin-W2-SW] *It almost feels like you're never gonna get on top of it because, by the time you maybe get on top of making a smart speaker safer, there'll be a new device …*
>
> [Adrian-W2-SW] *… and there's always* [unintelligible] *that people can make and … and bugs and stuff, like constantly being updated so you just never [able to keep up].*

In summary, the main barriers — as perceived by participants and based on their lived experiences of IPA — to preventing technology-facilitated abuse are:

1. a lack of confidence in their knowledge regarding smart home devices;
2. the complexity of managing data privacy across a multitude of devices and accounts;
3. the lack of support service preparedness in dealing with the ever-changing technology landscape.

These issues frame the problem context and ideas that participants generated during the ideation activity of the workshops. Accordingly, the next section sets out participants' co-created ideas for addressing intimate surveillance and abuse enabled by smart home devices.

THEME 5: PARTICIPANTS' IDEAS FOR ADDRESSING SURVEILLANCE AND ABUSE ENABLED BY SMART HOME DEVICES

In addition to identifying the main avenues through which smart home devices can be exploited for the purposes of intimate surveillance and abuse, participants co-created ideas for addressing some of these challenges during the ideation activity (see Section 4.2). This section details participants' ideas, which mainly operated on two levels 1) addressing gaps in survivors and professionals' knowledge of digital privacy through training and educational resources, and 2) ideas for improving the interpersonal privacy mechanisms of smart home devices.

DIGITAL PRIVACY TRAINING AND EDUCATIONAL RESOURCES

[Emily-W4-G4-SW] *I guess the big answer to all of this is just providing knowledge, isn't it?*

Overall, as illustrated by the transcript above, survivors and professionals felt that the main issue that needs to be addressed, regarding technology-facilitated abuse, is the gap in their knowledge regarding digital privacy management. As observed in Theme 4, professionals expressed the opinion that they do not possess the knowledge and training necessary to feel confident in supporting victims of technology-facilitated IPA, especially given the rapid pace of technological development. The transcript below illustrates this point, where professionals discuss the need for ongoing digital privacy training and practical advice that will enable them to better support victims. More specifically, participants are debating a lack in preparedness to address current issues related to social media privacy and spyware, demonstrating that training for IPA support workers has not kept pace with already widespread digital technologies.

[Jordan-W4-G2-SW] *I mean, I have like this idea in my mind that I want somebody locally to set up like a course, like you go on any IT course, and just talk me through …*

[Freya-W4-G2-SW] *… like with the stalking course …*

[Jordan-W4-G2-SW] *… yeah, talk me through Facebook, Twitter …*

[Freya-W4-G2-SW] *… yeah.*

[Jordan-W4-G2-SW] *… Instagram, you know.*

[Freya-W4-G2-SW] *Yeah.*

[Alex-W4-G2-SW] *Yeah.*

[Freya-W4-G2-SW] *'Cause I think there's so many things and you become aware of so many things and what you can do but it's keeping up with it all the time.*

[…]

[Jordan-W4-G2-SW] *But you know, how to put trackers on your phone, how to take them off, how to look for them and something that's particularly in our line of work that we can look for …*

Furthermore, professionals felt that current risk assessment procedures should be updated to effectively identify technology-enabled abuse. In the tran-

script below, a support worker describes how she fears that without an updated risk assessment questionnaire, victims may not disclose technology -enabled abuse. She discusses how the right questions may be essential in prompting victims to become aware of these forms of abuse, which could otherwise go unrecognised.

> [Ayana-W4-G3-SW] *In terms of empowerment, I mean I'd kind of see that as empowerment through universal education. But when we've got people coming into our services, it's maybe about a universal approach in doing that kind of checklist of, 'cause you know when we're building one of those support plans around need, we're very often led by survivors' need and what they tell us about what's happening but we maybe need to do that [digital] hygiene first and kind of, um, because you can't assume that they haven't got it [being covertly surveilled] because they don't tell us.*

In addition to training, participants expressed the need for a specialised support service to provide information and practical guidance on managing digital privacy for victims. The transcript below illustrates this idea and considers creating collaborations with IT experts to deliver the support.

> [Emily-W4-G4-SW] *But I think the idea of providing some sort of forum for women to be able to go and if we're talking about empowerment, to learn about how to do this. Yeah, face-to-face …*
>
> [Isabelle-W4-G4-SW] *… a service where for people who are experiencing domestic abuse could go to be made aware …*
>
> [Emily-W4-G4-SW] *… yeah, and that would need to be face-to-face, not technology because technology might be the issue in the first place. So someone who can sit with someone who can actually say "you know, this is what you can do" …*
>
> [Aailyah-W4-G4-SW] *… someone at college, maybe the students at college might be … I'm gonna do this, I'm gonna put this course on for my clients …*

Survivors expressed the same sentiment, discussing the need for support provision alongside IT specialists, to guarantee the accuracy of the information and guidance being delivered.

> [Leah-W5-G1-S1] *Yeah, I think I pose that questions because for individuals to have that level of understanding and keep up-to-date with it [technology], um, like you were saying, if you're in an abusive relationship, you may know exactly what's happening*

but you don't know how to tackle it. You go and talk to all these various services but they don't know how to tackle it. Um, should they be specialists in these services that we can actually contact […].

On the other hand, professionals also communicated the opinion that rather than attempting to address all of victims' privacy concerns through a specialised service, they should provide resources that enable victims to protect themselves on an ongoing basis. This would have the result of empowering victims by giving them the tools necessary to adapt to technological change and advancements, whilst reducing reliance on continuous support. The following transcript shows participants discussing an idea for an app that provides survivors with digital privacy information and alerts, in the form of short audio clips.

[Masha-W4-G4-SW] *Yeah but actually removing it all for her isn't empowering her, it's neutralising the problem but it's not actually empowering her. She needs to know what these things are so that she can …*

[Emily-W4-G4-SW] *… so what this lady wants is to have the knowledge to be able to act on this herself so she can take control about what's happening. So, we've got to think about yeah "how do we supply …"*

[Masha-W4-G4-SW] *… so you're saying that it just goes bing and then …*

[Sam-W4-G4-SW] *… to protect yourself from Snapchat, here's some ideas, you know what I mean?*

[Masha-W4-G4-SW] *Yeah, actually an audio recording!*

[Taylor-W4-G4-SW] *Yeah, that's not bad.*

These resources to support victims' in understanding digital privacy would be available outside of formal support and accessible to victims/survivors whenever needed. Furthermore, the type of information that survivors identified as being essential was generally very practical in nature. Or in other words, it took the form of easily understandable instructions aimed at accomplishing a specific goal, as illustrated in the transcript below.

[Mariam-W1-G2-SW] *So what further support and information would a victim need regarding this smartphone?*

[Esme-GW1-G2-S] *The turning locations off, privacy settings.*

[Daisy-W1-G2-S] *Mmmm [yes].*

[Esme-GW1-G2-S] *Passwords as well.*

[Mariam-W1-G2-SW] *[writing] "Turning location off, understand your privacy settings", yeah? See I'm thinking of spyware. If you've got spyware on your phone, that opens up a whole world. So [writing] "understanding privacy". What about if you think there is something on your phone? What would you like to happen, in an ideal world?*

Similarly, the next transcript further illustrates this point by discussing the need for practical and implementable instructions that can be leveraged to increase victims' safety as quickly as possible.

[Dana-W1-G2-S] *For security, yeah. Access on how to secure things to that people can't … I know it's silly things like put plasters over cameras that you shouldn't have to but support with that, to make someone feel safe.*

In summary, participants co-created ideas to address gaps in knowledge and support regarding digital privacy centred around:

1. technology-related training for support workers;
2. educational workshops for victims delivered in collaboration between support services and IT experts;
3. practical guidance and resources that victims/survivors can access wherever and whenever they need to.

IMPROVED INTERPERSONAL PRIVACY MECHANISMS FOR SMART HOME DEVICES

In addition to training and resources on digital privacy, participants co-created ideas aimed at improving the privacy afforded by smart home devices. The ideas that participants generated were related to the concerns outlined in Themes 1 and 2, regarding device logs, remote control of devices, and remote access to live feeds. Accordingly, participants' ideas focussed on questions of interpersonal privacy, or in other words, privacy between members of the same household. Participants' ideas have been grouped into four topics that are expanded upon below, namely, 1) device affordances, 2) multi-user support and permissions, 3) data maps, and 4) spyware removal. Each of these are discussed, in turn, below.

DEVICE AFFORDANCES & FEATURES

Devices such as indoor security cameras that enable remote access to live video and audio streams were extensively addressed in the ideation activity. Participants' design ideas largely focussed on improving awareness of when data is being recorded, for users inside the home. 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 are capturing audio, through more prominent visual or auditory cues. In the ensuing transcript, a survivor proposes that indoor security cameras should emit an audio cue, at regular intervals, when capturing video.

> [Eva-W1-G1-SW] *But then if you had a [indoor security] camera that like every hour had to beep, then you'd know if something was there.*

Participants also 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 the live video feed while another user is at home, the system should require an additional level of authorisation from the user in the home.

> [Erin-W2-SW] *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 …*
>
> [Amira-W2-SW] *Yeah.*
>
> [Erin-W2-SW] *You know and independently can say [yes or no] …*

Furthermore, an additional level of authentication (or authorisation) from a user inside the home could similarly be applied to devices that can be remotely controlled, such as thermostats or home hubs. An added level of authorisation would allow the user in the home a higher level of control over devices than users attempting to access the system remotely. Thus, safeguarding users in the home and addressing participants' concerns regarding remote control of devices and remote access to live feeds.

MULTI-USER SUPPORT + PERMISSIONS

Although smart home devices 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 (Amazon, 2018; Google,

2018). During the workshops, participants discussed issues surrounding the use of shared accounts and easy access to another user's account within the same household. For example, the former can 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 happen if users forget to switch between accounts before using a device.

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

> [Eva-W1-G1-SW] *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.*

Having a different account for each user can mean that participants' concerns regarding device usage logs (Theme 2) would be addressed, as each user would only have permission to view their own usage data.

"AWARENESS APP"/DATA MAPS

All participants expressed uncertainty as to where data is stored. As previously mentioned (see Theme 4), 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 or app updates.

> [Mariam-W1-G2-SW] *I think what would be good would be some kind of um … 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.*
>
> [Maria-W1-G2-S] *Problem with that is when you update your things it goes back to basic, so you have to turn everything off again.*
>
> *[…]*

[Mariam-W1-G2-SW] *But then if you could just like press something and it said "this is what's going on with your world at the moment, in terms of IT …"*

[Dana-W1-G2-S] *"… do you want your location on or off?" They should say it. When you update it, they should have that button …*

[Maria-W1-G2-S] *Especially if it is off already. If it's not then …*

[Dana-W1-G2-S] *… then fair enough. But if that button's off they should let you know, make you aware that that's gonna go back on when updating.*

[Maria-W1-G2-S] *Yeah.*

[Dana-W1-G2-S] *And they don't.*

Additionally, this "awareness app" would display a list of locations from which the user's data has been accessed. Using this list, victims can review who may be accessing their data beyond themselves and other trusted users.

[Sayeeda-W4-G3-SW] *And do you know, do you get, I don't know whether there's a potential that at any point in the distant future where you could even see a report on your own stuff, where it could show you where your things have been accessed from?*

[Nantia-W4-G3-SW] *Wouldn't that be good?*

[Group] *Yeah. […]*

[Sayeeda-W4-G3-SW] *Yeah! Who's accessed, and at what time, and what device for your accounts. It would be like a [phone] statement.*

A centralised visualisation of data gathered by all of a user's devices, alongside where it is stored and who has access to it, addresses participants' concerns regarding their understanding of the cloud. This is accomplished by taking all of this metadata and turning it into an easily readable visual format, thereby, removing some of the complexity in understanding data capture, sharing, and access across multiple devices and accounts.

SPYWARE REMOVAL

During the workshop, participants expressed difficulty in detecting spyware and a general concern over the means through which spyware could be installed in the first place (see Theme 2). Participants equally feared that spyware would progress beyond

smartphones and move onto devices such as smart home hubs, TVs, etc. To address this issue, built-in spyware detection software was proposed.

> [Mariam-W1-G2-SW] *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]?*
>
> [Erin-W2-SW] *And some sort of like anti-spyware for it [home hub]?*
>
> [Amira-W2-SW] *Mmmm [yes].*
>
> [Amira-W2-SW] *Just "Alexa, run spyware scan".*

Built-in spyware detection is intended to address participants' fears that legitimate smart home devices, such as an Amazon Echo, be exploited for the purposes of covert monitoring. Spyware detection and removal would prevent software design to covertly record/stream audio from running in the background, much in the same way that anti-virus software operates on laptops.

To summarise, this theme outlines participants' ideas for addressing technology-enabled IPA through smart home devices. Participants' ideas were twofold:

1. improved training and educational resources on technology-enabled IPA and privacy management;
2. improved smart home device mechanisms that prioritise interpersonal privacy within a household.

4.3 DISCUSSION

The codesign workshops with survivors and support workers were structured with two aims in mind. The first was to understand participants' main concerns regarding surveillance and abuse in the context of near-future smart homes. The second was to engage participants in co-creating solutions to support victims of surveillance and abuse enabled by smart home devices.

Regarding the first aim, the scenarios that participants generated in the workshop show they are mainly concerned that smart home devices will be used for IPA in the following ways:

1. shared device usage logs can be used by perpetrators to infer information such as when a victim is at home or not;

2 remote video and audio feeds that enable real-time surveillance of victims inside their homes;

3 remote control of smart home devices, which can be used by perpetrators as a tool for *gaslighting,* harassment, and creating fear.

Participants' scenarios for how smart home devices can be misused for surveillance and abuse aimed to predict the near-future of ubiquitous smart homes, and are based on their real-life experiences of IPA. Although aiming to predict the misuse of smart home devices within a near-future context, most of participants' scenarios reported on in Themes 1 and 2 are technically feasible using existing commercial devices. Examples include monitoring a user in the home via live security camera feeds or inferring when a user is in the house by the current thermostat settings. They are feasible due to the fact that such systems are often designed with an "idealised" family unit in mind (Desjardins *et al.,* 2019), where trust between household members is assumed to be a given. Therefore, smart home devices tend towards a default of sharing data between household members and allowing for remote access/control of devices, even when another user is in the home. This makes them ill-suited for living situations in which trust between household members is not guaranteed, such as in the case of IPA.

This work with survivors of IPA highlights the dangers of current smart home design operating within its existing limited scope. Designing solely for contexts in which it is assumed that members within a household are not concerned with interpersonal surveillance, renders it extremely difficult for users to safeguard their privacy when necessary. Inadequate privacy controls exacerbate the complexity of managing personal privacy, which was identified as an already overwhelming task by participants. In fact, an analysis of the workshops revealed that participants regarded smart home devices as a threat due to mainly two underlying reasons, namely 1) a lack of confidence in their knowledge of managing complex privacy controls, and 2) a lack of trust in support organisations' ability to provide effective guidance on digital privacy. Freed at al., (2017) point out similar concerns in their work with survivors and support workers investigating current technologies such as smartphones and social media.

In this context, participants identified *non-use* as the most effective strategy to protect themselves. Even though the social and economic consequences of opting-out of using digital technologies were recognised, survivors still felt that the complexities of managing digital privacy were too many to effectively handle. Unsurprisingly, when asked to generate solutions to prevent smart home devices being used for abuse,

participants largely focussed on 1) training and guidance on digital privacy management for survivors and professionals, as well as 2) improved interpersonal privacy mechanisms for smart devices.

Regarding training and guidance, participants suggested technology-specific training for professionals and educational workshops for victims, which would be delivered in collaboration with IT experts. Participants also outlined the need for digital privacy management resources that can be accessed outside of formal support services. These would take the form of short video or audio clips outlining instructions that victims could easily follow to accomplish specific goals, such as changing an iCloud password. In addition to privacy management resources, participants also co-created ideas that directly address the interpersonal privacy afforded by smart home devices. Participants' ideas included more robust support for multi-user accounts, in which devices automatically identify different users and assign them personal accounts. This served the purpose of avoiding centralised historic usage logs from which information about users in the home could be inferred. Co-generated ideas also addressed real-time remote access and control of smart home devices. Participants proposed that all requests for remote access be authorised by the user inside the home, assigning higher levels of system permissions to users inside the home as opposed to those accessing it remotely.

The balance between the commodity and usefulness of smart home devices versus users' privacy preferences has begun to be discussed in fields such as gerontechnology, where it was widely assumed that home technology developed to keep the elderly safe in their own homes would be welcomed. However, research has found that users' willingness to adopt such technologies depends on many factors including privacy, especially who can access which data (e.g., family members) and in what detail (Shankar *et al.,* 2012). Research within *non-traditional* households indicates that smart home technologies need to be designed with human agency in mind and that a broader set of users need to be considered in the design process. The design of smart home devices requires careful consideration of how technology mediates, influences, and contributes to human relationships.

This work aimed to engage survivors in anticipating the threats posed by the near-future ubiquity of smart home appliances, to inform their design with the goal of preventing misuse. In this context, the methods used in the workshops, which prompted participants in envisioning near-future scenarios based on their lived experience of IPA, were successful in identifying potential future-threats for victims of IPA. The videos served

the purpose of both informing participants on existing visions of what data sharing between intimate partners within smart homes could be, but also to contextualise daily living activities within a near-future paradigm. Similarly, the *scenario creation* and *data mapping* activities allowed participants to build on their lived experience, by grounding the activities around *personas* who are victims of IPA, whilst transporting those experiences to a near-future imagined scenario of smart homes. Finally, the *ideation* activity enabled participants to imagine near-future scenarios in which their concerns regarding smart devices are addressed.

In this sense, envisioning near-future threats can be useful to the ongoing design of smart device privacy and security mechanisms, by anticipating the treats such devices can pose within IPA contexts if their design goes unrevised. Although speculative in nature, it is important to keep in mind that participants created these scenarios based on their lived experience of IPA, or their experience of supporting victims of IPA.

IPA survivors and support workers have not been previously included in the process of anticipating the potential threats posed by novel technologies. Existing research on technology-enabled IPA has focussed on the challenges currently facing victims, such as social media, location services, and email, through interviews and focus groups (Southworth *et al.,* 2007; Marganski and Melander, 2015; Matthews *et al.,* 2017; Freed *et al.,* 2018; Harris and Woodlock, 2018). This work extends current knowledge by bringing survivors and support workers into the process of 1) designing improved support for victims and survivors, as well as 2) contributing to a wider discussion on smart home interpersonal privacy. In addition, the work contributes to the codesign field by outlining a collaborative design process, within a highly sensitive context, alongside survivors of IPA.

4.4 ROLE OF THE PRACTICE

Within the context of the codesign workshops, the role of my practice was essentially three-fold:

1. as a designer, my role involved creating materials to support the workshop activities, which functioned as scaffolding that provided the context necessary for participants to engage with, discuss, and speculate on the near-future of smart home technologies;

2. as a facilitator and a researcher, my role included ensuring all participants had the opportunity to contribute and the environment was a caring and respectful

one, where power dynamics between me, the support workers, and survivors were as balanced as possible;

3 as a designer and a researcher, a process of *infrastructuring* the project by building relationships with support workers and reviewing designed workshop materials in collaboration was fundamental to the success of this PhD work.

In terms of points 1 and 2 above, participatory design has long been committed to the design of processes that promote and enable participation of multiple contributors and stakeholders (Robertson and Simonsen, 2012; Bardzell, 2018). The design of the workshops materials the activities themselves, as well as the facilitation of such workshops, were an integral part of my design practice within this PhD.

Furthermore, the use of visual materials to explain abstract concepts such as smart homes and to scaffold the workshop activities allowed participants to engage with the topic in a way that other purely verbal or written methods do not. A verbal or textual explanation of concepts such as surveillance and smart homes may not be as effective as telling a visual story that illustrates those concepts in concrete objects and actions. In the same way, the cards used in the ideation activity gave participants a series of physical artefacts that they could shuffle, distribute, share, and use at any point for inspiration and discussion. Artefacts in codesign workshops have been shown to provide a common ground for communication between participants, stimulate the exchange of opinions and perspectives, as well as mediate the creation of new ideas (Halskov and Dalsgaard, 2007; Andersen and Mosleh, 2020).

Finally, addressing point 3, for the workshops to be a comfortable and safe space for all those involved, a great deal of planning and collaboration with NGOs was necessary. Support workers from DVIP reviewed the workshop materials with me and we modified them together, intending to ensure that none of the activities would be triggering for survivors. Support workers also took charge of inviting participants, explaining the research to them, and ensuring that participants understood what to expect from the workshops before any contact between myself and potential participants was established. As referred to in Section 1.5, to build a relationship of trust and collaboration with the support workers, a lengthy process of *infrastructuring* (Björgvinsson, Ehn and Hillgren, 2010) this PhD work through volunteering and training was necessary. Within the field of participatory design, and more importantly social design, I believe this process of *infrastructuring* is essential, if not part of, the design practice itself.

4.5 CONCLUSION & NEXT STEPS

In line with the aims (1 & 3) and objectives of this PhD work (Section 1.3), during the codesign workshops, participants identified a series of viable threats posed by smart home devices, related to remote access of live feeds, remote control of devices, and shared device usage logs. Underlying many of these concerns was participants' lack of confidence in their own knowledge of digital privacy management, as well as the fact that support services are not equipped to deal with technology-enabled abuse. The complexity of managing privacy settings across smart home devices, in addition to participants already existing personal devices, was seen as overwhelming and generally unachievable with their current levels of privacy management knowledge.

Accordingly, the idea that was most widely discussed, by participants in the workshops, was that of creating digital privacy and security training and guidance for survivors and professionals. Based on this finding, and working alongside Refuge, we collaboratively decided to prototype a chatbot that responds to victims' queries regarding digital privacy and security mechanisms. A chatbot was selected for several reasons:

- It is available 24 hours a day, seven days a week, meaning that survivors can access it whenever they need to;
- It can deliver responses in the form of short videos with visually illustrated instructions that victims can follow on their own devices;
- Content can be easily extended to several languages.

In this way, the codesign workshops responded to the aims and objectives of this work by:

- Presenting a series of workshop materials and activities appropriate for working alongside survivors of DA;
- Evidencing that codesign can be an effective method for creating "solutions" alongside survivors and support workers.

The next chapter discusses the chatbot in further detail, including design, technical specifications, features, development, and testing.

5

CO-DEVELOPMENT: CHATBOT CONCEPT, DESIGN & IMPLEMENTATION

This chapter begins by describing the process of developing a chatbot in collaboration with Refuge, as a response to the findings from the interviews (Chapter 3) and codesign workshops (Chapter 4) with survivors and support workers. The chapter then progresses onto the design and technical implementation of the chatbot, followed by a discussion of the co-development process. The aims of this chapter are to recount:

- the process of developing the concept, which led to a chatbot, in response to the themes that emerged from the codesign workshops;
- the design and technical development of the chatbot and its content (the instructional videos);
- the process of transferring co-ownership of the chatbot from me, as a designer, to ownership by the community.

Chatbots, also known as conversational agents, are programs designed to simulate human conversation via text between a human and an artificial agent (Janarthanam, 2017, p. 8; Batish, 2018, p. 3). The chatbot described in this chapter was designed to assist victims/survivors in managing their digital privacy settings across social media (Facebook, Instagram, Snapchat, and Twitter), Whatsapp, Google Maps, and Apple ID. The bot presents a series of initial options to users, such as Location Settings, Social Media, Whatsapp, and then allows users to drill down to more specific information needs, such as how to *block* another user on Facebook. Once the user has identified the specific piece of information they require, the chatbot responds with an animated video containing instructions on how to modify those specific settings or perform a particular task (Fig. 14).

The chatbot, at the time of writing this thesis, is hosted on Refuge's website1. Refuge is one of the largest charities in the UK providing support and emergency accommodation for victims and survivors of DA (Refuge, 2017). Therefore, Refuge is well-positioned to take ownership of the output of the codesign process, to deploy it in a real-world setting, and to assume the ongoing responsibilities of maintenance and updates beyond the lifespan of this PhD. Refuge, as a community partner in the codesign, has taken full ownership of the chatbot and launched it alongside its new helpline website in December 2019. The chatbot will be referred to, hereinafter, as either the *Bot* or the *Refuge Bot.*

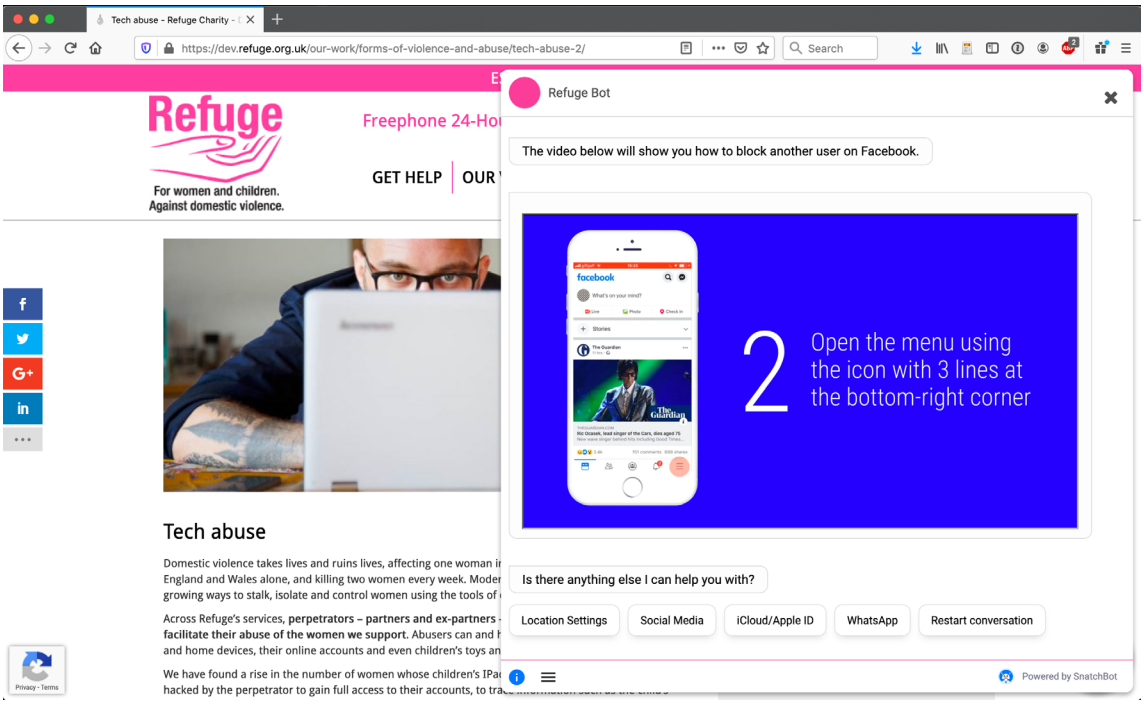

Fig. 14. *Refuge Bot* displaying an instructional video on how to *block* another Facebook user on an iPhone.

In terms of process, this last phase of codesign with Refuge progressed according to 4 main stages during the course of 10 months. Stage 1 involved collaboratively developing and refining a design concept based on the findings from the codesign workshops and interviews. In stage 2, the concept was implemented and then collaboratively evaluated in stage 3 (Chapter 6). Finally, in stage 4, Refuge took ownership of the codesign output and released the chatbot to the public.

Below, a description of the chatbot co-development with Refuge is followed by further detail on 1) the technical development platform, 2) the chatbot content and voice, 3) the chatbot design & information architecture, and finally, 4) the process by which

1 https://dev.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/

Refuge has assumed ownership of the chatbot for deployment on their website. The chapter closes with a discussion, future work, and conclusions.

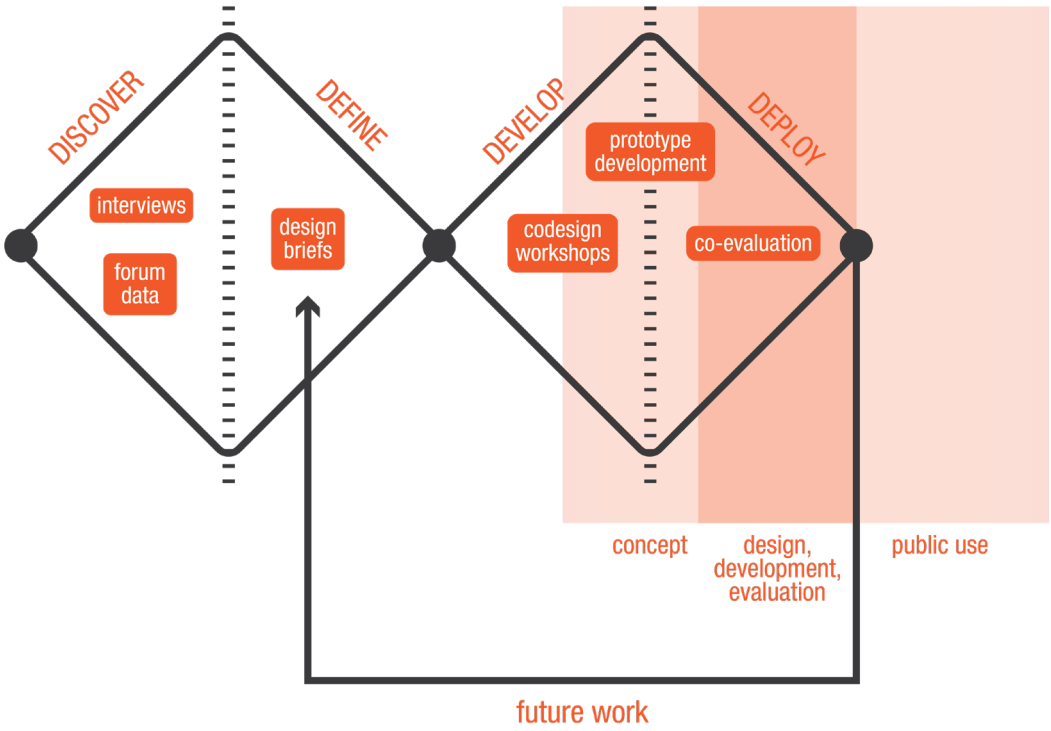

Fig. 15. Refuge Bot's development lifecycle imposed on the double diamond methodology

5.1 CONCEPT CO-DEVELOPMENT

Once an analysis of the findings from the interviews, forum data, and co-design workshops had been performed, and to progress the process of codesign, I sought to engage with Refuge as a community partner in the co-development phase. Refuge's position as one of the biggest UK charities support victims of DA means that — as a result of a partnership between this research and Refuge — the output of the codesign process would have the potential to reach a wide range of victims and survivors in the UK. Furthermore, Refuge collaborates internationally with the National Network to End Domestic Violence (NNEDV), who are based in the US and have published a considerable amount of guidance for victims on technology-facilitated IPA (NNEDV, 2019). For these reasons, I identified Refuge as a potential further collaborator for the final stages of the codesign process. Although my previous collaborations had been with DVIP, VS, Norfolk local authority, and Changing Pathways, these institutions are smaller and, as highlighted by themselves, too constrained in terms of staff, time, and budget to take ownership of a codesigned output. For these reasons, a novel

partnership was sought and established with the consent of all those involved. It was through the contacts at NNEDV that an initial meeting with Refuge was arranged. The initial meeting aimed to:

- Discuss the findings from the interviews (Section 3.7) and workshops (Section 4.3), particularly participants' needs and ideas for solutions;
- Discuss whether there was an interest in progressing the codesign in collaboration with Refuge's management, support workers, and survivors;
- Discuss which of the themes/ideas (Section 4.3) should be progressed further and how this process would be shared collaboratively;
- Discuss future ownership and maintenance of the output.

During the meeting, Refuge expressed great interest in developing staff and survivors' knowledge regarding digital privacy and security. Refuge was specifically interested in empowering support workers and victims to manage digital privacy more effectively, which aligns with Theme 5 — *Digital Privacy Training* and *Educational Resources* — from the workshops (Section 4.3). Theme 5 outlines survivors' ideas for developing learning materials and training on digital privacy management. In this context, Theme 5 emerged as the theme that would be addressed in this final stage of codesign.

As the workshop ideas and Theme 5 were refined with Refuge staff, throughout this co-development phase, the concept of a chatbot was put forward as a means of delivering knowledge to victims/survivors on digital privacy management. The idea of a chatbot was based on the notion that, as an automated system, it would be capable of delivering information without further constraining support workers' time, whilst being accessible from anywhere at any time. The chatbot would deliver instructional videos showing victims how to manage their privacy settings on several platforms across Android and iOS. As part of the action-points resulting from the meetings with Refuge, I was tasked with developing the concept further and investigating the feasibility of building a chatbot within the PhD's timelines. The Head of Operations at Refuge was responsible for discussing the concept with frontline workers and survivors, in order to gather their opinions and reflect on the appropriateness of the concept.

To gather survivors' opinions and thoughts regarding the idea of a chatbot, Refuge frontline staff conducted interviews with 8 survivors and focus groups with 30 survivors living in Refuge shelters (see report in Appendix E). In the findings report, the conclusion

states that *"[t]he survivors consulted overwhelmingly felt that it was a good idea for Refuge to add a chatbot to their website".* The report also shows that survivors felt it was important that the chatbot was only used to deliver technical support and did not replace face-to-face interaction with support workers on matters such as emotional support and safety planning. Participants also appreciated the chatbot as a "silent" form of technical support when they need it the most and when a support worker is not available. Additionally, survivors highlighted that:

- visual instructions, rather than complex text-based instructions, would be most useful for a topic such as digital privacy management;
- the chatbot needs to be accessible on mobile devices as these are often the technology that survivors have access to;
- the chatbot should include information on how to contact a human support worker in case the survivor/victim wishes to do so.

Based on the findings from Refuge's interviews and focus groups with survivors, over the following weeks, several meetings were conducted to develop the chatbot concept collaboratively alongside Refuge. The meetings included Refuge's Head of Operations, frontline support workers, staff from the communications and media team, and me. A final concept was agreed upon which can be described as:

> A chatbot on Refuge's website that provides technical support to victims/survivors seeking information on digital privacy & security. The chatbot does not aim to replace interaction with support workers on matters such as safety planning and emotional support but, rather, to provide easily accessible technical guidance. The chatbot will deliver information via animated instructional step-by-step videos. Videos will address digital privacy and security on common social media apps, location services, and instant messaging (IM) apps, across iOS and Android.

Lastly, the chatbot does not at this point include information on managing digital privacy on smart home devices. In collaboration with Refuge, it was decided that releasing such information to the public may be premature as perpetrators could learn from the content intended to support victims. Refuge have planned to update the chatbot with information on different smart home devices as the need increases and becomes more mainstream. The architecture of the chatbot (see Section 5.3) is flexible and easily extendable to include novel content around as many topics as necessary, which renders it adaptable to novel survivor needs that Refuge may uncover over time.

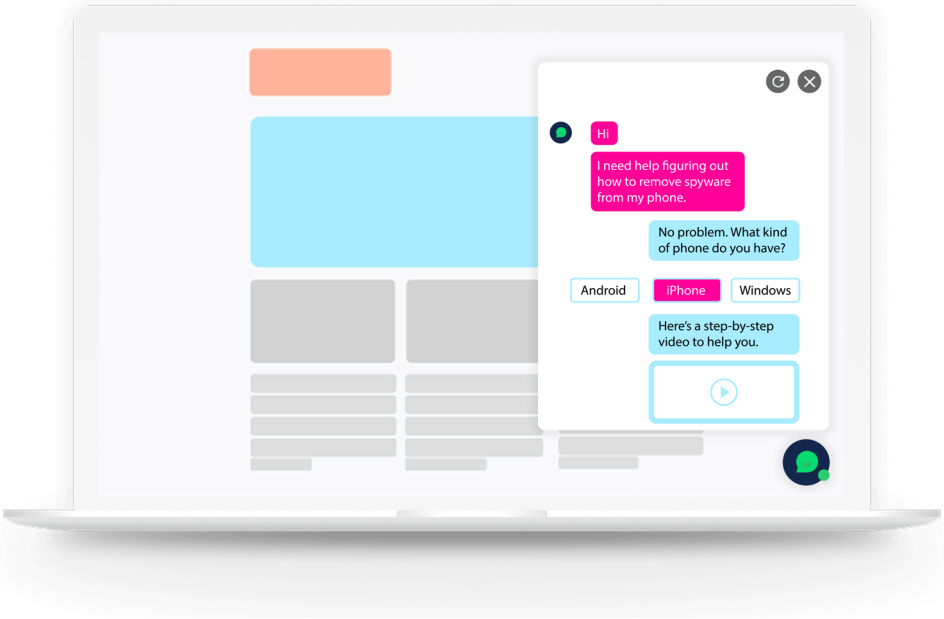

Fig. 16. Initial mockup of the concept

5.1.1 THE USE OF CHATBOTS IN SENSITIVE CONTEXTS

The concept of the chatbot was also informed by the existing use of chatbots within sensitive contexts, such as mental health support, medical triage, and reporting sexual harassment (Fitzpatrick, Darcy and Vierhile, 2017; Babylon, 2019; Spot, 2019). It has been argued that chatbots, or text-based conversational agents, have the potential to democratise access to information and services by being readily and remotely available from anywhere on common devices and platforms (Følstad *et al.,* 2018). In this way, chatbots can provide instant and anonymous access to information from wherever the user is located, making services more accessible, available, and affordable (Cameron *et al.,* 2018). Furthermore, the anonymous nature of chatbots is thought to be an advantage in certain contexts, as previous studies have found that users are often more comfortable seeking sensitive information through a chatbot rather than in conversation with a real human (Mindshare, 2016). In fact, chatbots are being deployed within mental health contexts because they are a means through which instant, anonymous, and always-available support can be delivered (Cameron *et al.,* 2017). For example, the cognitive behavioural therapy chatbot called *Woebot* was found to be effective in reducing symptoms of depression and anxiety amongst college students (Fitzpatrick, Darcy and Vierhile, 2017). *Babylon Healthcheck* is providing medical triage (Babylon, 2019), and *Florence* offers mental health-promoting behaviour change (PACT Care BV, 2019).

Similarly, chatbots are being explored by several organisations as a means to support victims of DA. For example, *Jael.ai* aims to coordinate care for victims attempting to flee an abusive relationship by organising a refuge and taxi to pick victims up from their homes (Axiom88, 2016). *Hello Cass* provides information on locally available DA services, safety planning, and the legal system (Good Hood, 2019). *rAInbow* provides information on signs of abuse in a relationship and shares personalised DA-related stories with the aim of helping those going through abuse (AI for Good, 2018). As with *Refuge Bot*, these bots aim to provide information and very specific practical support (e.g., booking a taxi) rather than replace the emotional support and advice offered by professional support workers, acknowledging the limitations of artificial intelligence's capabilities to react appropriately and sensitively to victims' emotional support needs. Although chatbots cannot understand the nuances of users' life history and current circumstances, and therefore are inadequate to replace face-to-face interactions with trained professionals, they are an effective mechanism for delivering information (Kretzschmar *et al.,* 2019).

All of the above examples can be seen as chatbots developed for a social purpose, from health screening to mental health, and DA. Følstad *et al.* (2018) propose classifying *chatbots for social good* according to three categories 1) *chatbots for autonomy,* 2) *chatbots for competence,* and 3) *chatbots for social relatedness.* The second category — *chatbots for competence* — is the one in which the *Refuge Bot* sits. Chatbots for competence are defined as those that provide users with the support and materials needed to develop a particular skill or competency (Følstad *et al.,* 2018). In this case, the *Refuge Bot* offers victims/survivors streamlined access to a series of videos on how to manage their digital privacy settings across social media platforms, IM apps, and other location-based services on both Android and iPhone. Furthermore, the *Refuge Bot* provides support in cases when the Refuge run National Domestic Violence Helpline may be unavailable or too busy. It releases support workers' time with clients for safety planning and other practical support beyond digital privacy concerns. What is more, as highlighted in Refuge's findings from the focus groups and interviews with survivors, step-by-step instructional videos may be a more effective and easier-to-understand form of delivering such content, as opposed to verbal instructions delivered over the phone. In this manner, the *Refuge Bot* is seen as supporting a number of advantages:

- instant and always available information that victims/survivors can access remotely and in an autonomous manner;

- information delivery in a format that is more adequate to the nature of the content and, therefore, eases comprehension;
- releasing helpline and support workers' time to focus on other aspects of service delivery;
- empowering victims/survivors with resources outside of formal support delivery.

The following sections will now describe the design of the *Refuge Bot* and its technical development in more detail.

5.2 CONVERSATIONAL DESIGN

An integral part of conversational agents is their *tone-of-voice* or personality (Shevat, 2017, p. 40). Shevat (ibid.) argues that a chatbot's personality should be aligned with its purpose as well as be context-appropriate and sensitive to users' needs. Sensitivity and appropriateness to context are especially relevant for a bot designed to interact with survivors of domestic abuse, where the correct *tone-of-voice* and messaging are essential to ensure a safe and sensitive interaction.

Moore at al. (2018) describe three basic conversation design principles. The first, *Recipient Design,* states that conversation should be tailored to match users' level of understanding. The second, *Minimization,* means that interaction should be kept as short and simple as possible. Finally, *Repair* states that the bot should be capable of recovering from failures. The bot developed as part of this PhD work addresses these three principles in the following ways:

- *Recipient Design.* Technical language and jargon related to digital privacy have been removed, wherever possible. The bots' messaging and use of language was informed by my experience of the interviews and workshops with survivors, as well as by existing literature on conversational design (Moore and Arar, 2018). Language was then evaluated in the co-evaluation with survivors and, finally, Refuge staff performed a last revision of the language before the launch (see Chapter 6).
- *Minimization.* The bot's content structure is limited to three levels of navigation and users are presented with available options at opportune moments during the interaction. Firstly, a simple navigation structure reduces the level of effort required for users to construct an accurate mental model of the bot's content

architecture. The navigation was co-evaluated and further refined in the evaluation process (Chapter 6). Secondly, presenting available options removes the need for users to guess what the bot is capable of providing information about.

- *Repair.* The bot allows users to correct input by either navigating back to the main menu or restarting the conversation.

Finally, regarding *tone-of-voice,* the name of the bot — *Refuge Bot* — was chosen for two reasons. Firstly, it clearly communicates that users are interacting with an automated conversational agent and not a human. Secondly, by giving the bot the name of the charity, we are not attempting to anthropomorphise it in any way. This was done to clearly communicate that the bot is automated and available to answer technical questions, rather than provide emotional or other practical support that is expected to be delivered by a human.

5.3 INTERACTION DESIGN & INFORMATION ARCHITECTURE

The design of chatbots marks a transition, for designers, from designing visual layouts and user-interactions to designing conversations between automated text-based conversational agents and users (Følstad and Brandtzæg, 2017). The Nielsen Norman Group (NNG) classifies chatbots according to two categories: 1) customer-service chatbots, and 2) interaction bots (Budiu, 2018). Interaction bots are those that provide an additional channel of interaction for users, beyond customer service. The Refuge chatbot is, therefore, an interaction chatbot as it provides an additional channel for accessing digital privacy management content on the Refuge website. What the Bot does is it essentially performs 'navigational triage' by enabling survivors to locate the digital privacy management content they are seeking in a guided manner.

The Bot leverages pre-determined responses, in the form of buttons (Fig. 18) to assist users in locating information. The pre-determined categories (Fig. 17) provide users with an overview of the content offered by the chatbot, which can be especially useful for first-time users who do not already know what to expect nor what the chatbot can be used for. Thus, the structure of the chatbot can be described as a linear flow, which has been designed to guide the user through a limited number of tasks. The overall structure is a decision tree with suggested responses, at specific points in the tree, which determine routing to subsequent conversational nodes. Or in other words, the

bot asks a question and then users' answers serve as a trigger to advance the bot on the correct branch of the flow (Budiu, 2018). For example, if a survivor was using the bot to find a video with instructions on how to turn off location services for Snapchat on an iPhone, the linear flow would be:

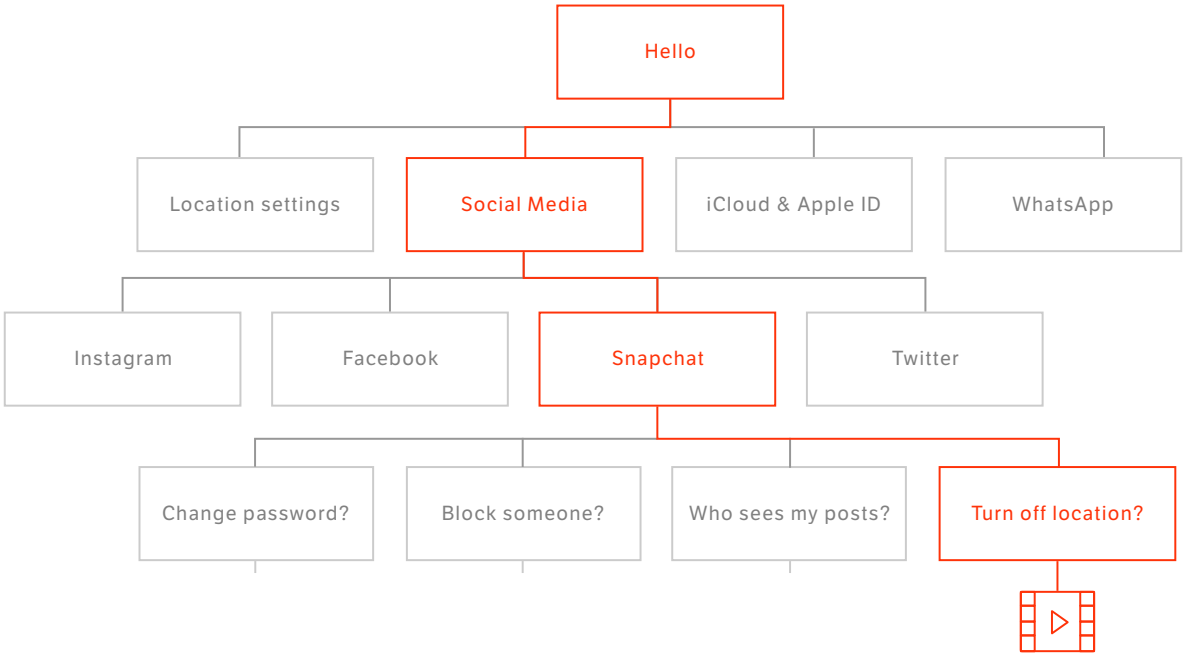

Fig. 17. Conversation journey leading to an instructional video on how to disable Snapchat's use of location

The following subsections describe the chatbot's onboarding process and information architecture design in more detail.

5.3.1 ONBOARDING

Onboarding is the term used to refer to the first interaction users see from a chatbot (Shevat, 2017, p. 80). During *onboarding,* the bot should make its purpose and functionality clear to users (ibid.). Regarding *Refuge Bot*, users' interaction begins with the following automated message and question:

> *Hello! I'm not a real human but I was created to help you to use your smartphone safely. If you're worried someone might be monitoring your mobile, I can help you change your settings to stay safer.*
>
> *I can help you secure your location on your phone, change your settings for social media (Facebook, Instagram, Snapchat, and Twitter), WhatsApp, and guide you through some other safety options on your iPhone and Android phone.*

If you're in danger and need to speak with a person, please call 999 or our Freephone National Domestic Abuse Helpline on 0808 2000 247.

Otherwise, please select one of the options below.

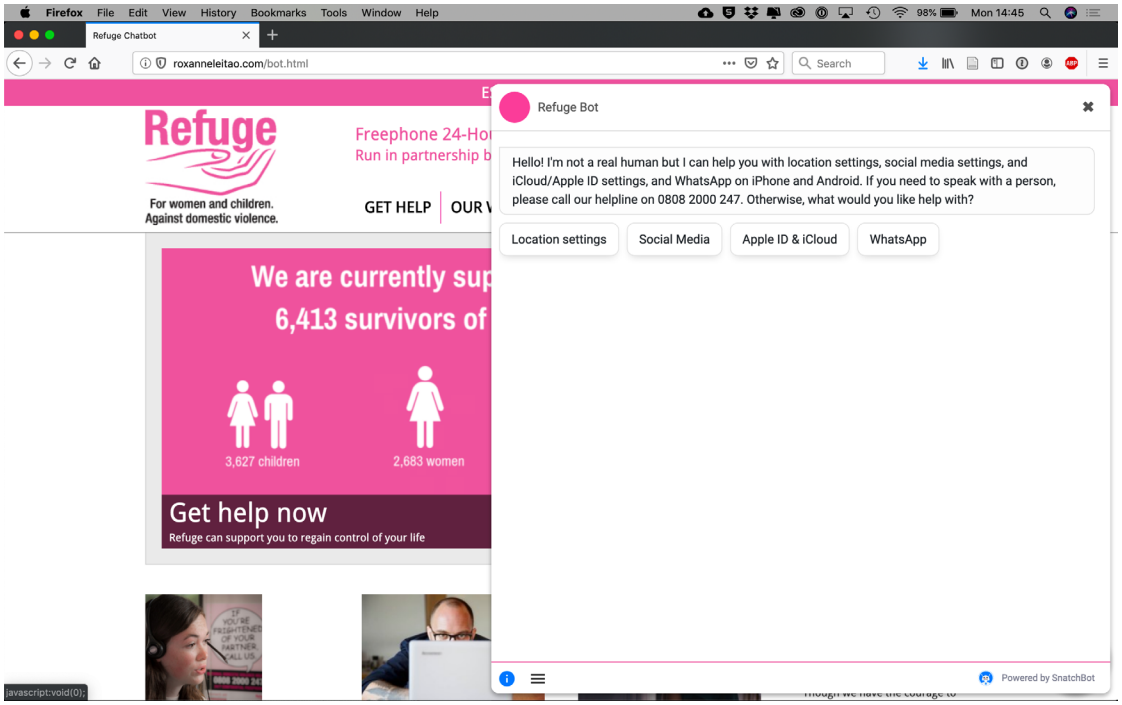

Fig. 18. *Refuge Bot's* onboarding message and buttons

In conversation with Refuge, we felt it was important for the bot to make it clear that users would not be interacting with a human agent from the outset. This is consistent with NNG's findings from a user-evaluation of interaction chatbots (Budiu, 2018). Therefore, the bot discloses its automated nature in the greeting statement, followed by the National Domestic Violence Helpline phone number in case users need to speak with a human.

If users chose to continue interacting with the bot, they can select one of four initial options: 1) *Location settings,* 2) *Social Media,* 3) *Apple ID & iCloud,* and 4) *WhatsApp* (Fig. 18). These four options immediately give users an overall idea of the capabilities of the bot and what kind of support is on offer, making the core functionality of the bot clear.

Once users have made an initial selection, the onboarding process is complete. As previously mentioned, the bot then adopts a decision tree structure, which is described in further detail below.

5.3.2 INFORMATION ARCHITECTURE DESIGN

The conversation has been designed to be a task-led conversation, or in other words, the conversation has been designed to help users complete the task of finding the digital privacy information they are looking for. Take as an example a user who is seeking a video related to location sharing on the Find My Friends app. Given that the chatbot currently hosts 33 videos, displaying all available videos in a list would not be the most effective way of enabling users to locate the information they are seeking. For this reason, content was grouped into categories and sub-categories that correspond to the menus and sub-menus displayed by the chatbot. Users work their way through the content by making choices when each menu or sub-menu is presented to them, at different points in the conversation with *Refuge Bot.*

The initial options presented to users, or in other words the top-level navigation (Fig. 19), outline all topics covered by the chatbot. Initially, it had been agreed with Refuge that the Chabot would cover 1) *location services,* 2) *social media,* and 3) *iCloud & Apple ID.* However, during the co-evaluation of the chatbot (see Chapter 6) it became clear that support for *WhatsApp* was also needed and was, therefore, added to the top-level navigation at a later stage. Currently, the top-level menu contains four categories (Fig. 18). Once a user has selected a top-level menu item, the chatbot then prompts them to choose whether they have an Android phone or an iPhone. As seen in Fig. 19, once a user has selected either iPhone or Android, the rest of their path is customised to that particular mobile operating system (OS) and they do not need to reselect their type of phone again. This is aligned with existing heuristics on chatbot design, which advise that bots be capable of remembering user-input, rather than asking users to re-enter the same information more than once (Shevat, 2017, pp. 52–54).

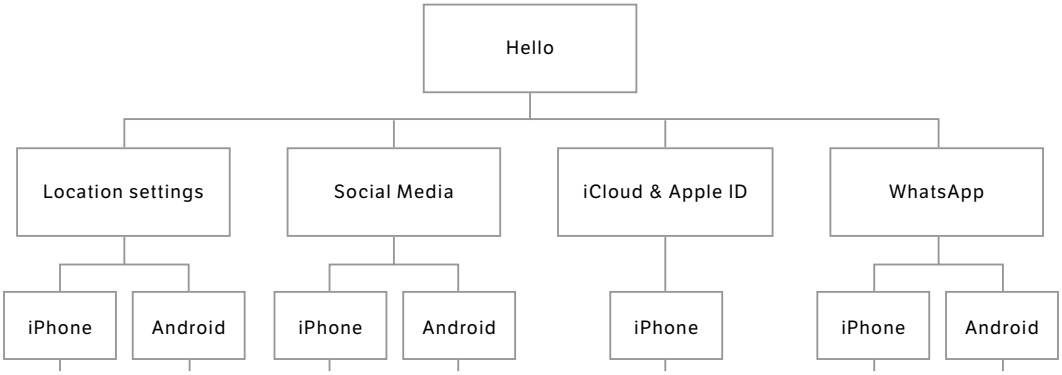

Fig. 19. Top-level menu structure and mobile OS selection

Each of the 4 top-level menu items — *Location Settings, Social Media, iCloud & Apple ID,* and *WhatsApp* — will now be expanded upon, in turn, below.

LOCATION SETTINGS

As seen in Chapter 4, one of victims' main concerns related to technology-facilitated IPA was location settings. Therefore, the first menu-item is *Location Settings* and all videos related to managing an application's access to location data are hosted within the *Location Settings* top-level menu item (Fig. 20). This includes social media apps, even though there is overlap between these and some of the videos listed under the *Social Media* menu item. The decision to have videos about location services hosted under more than one top-level menu item was made during the co-evaluation sessions (please see Section 6.4 for further detail), to make information as readily accessible as possible by replicating users' mental models of where the information should be located. In this manner, a user can, for example, find a video on how to disable location sharing for Instagram both under *Location Settings* or under *Social Media.* Fig. 20 below outlines the content available under the *Location Settings* top-level menu item.

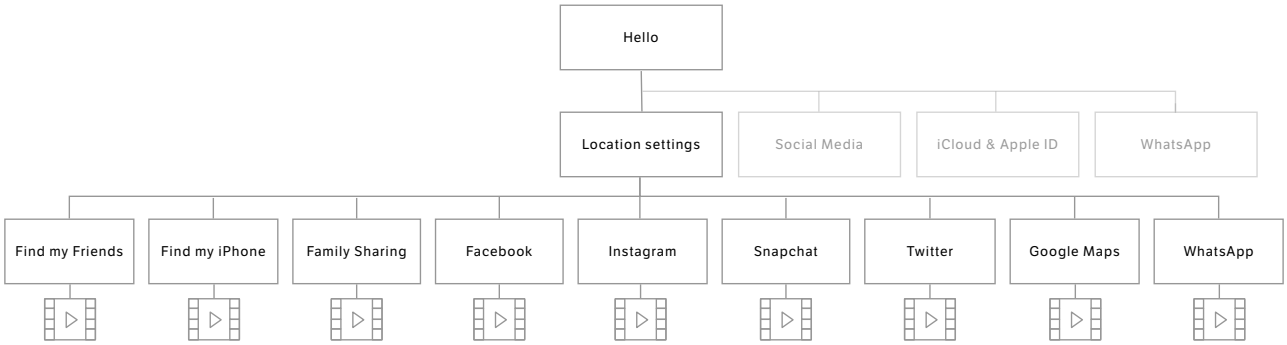

Fig. 20. Example of a second-level menu structure

Each second-level item, as seen in Fig. 20, leads to an instructional video. A complete list of videos found under *Location Settings* is as follows:

- Facebook location settings (iPhone and Android);
- Snapchat location settings (iPhone and Android);
- Twitter location settings (iPhone and Android);
- Instagram location settings (iPhone and Android);
- WhatsApp location settings (iPhone and Android);

- Google Maps location settings (iPhone and Android);
- Find my iPhone (iPhone only);
- Find my Friends (iPhone only);
- Family Sharing (iPhone only).

SOCIAL MEDIA

Unlike the *Location Settings* top-level menu, the *Social Media* menu contains a second-level menu (Fig. 21), which holds the following subcategories: 1) Instagram, 2) Facebook, 3) Snapchat, and 4) Twitter.

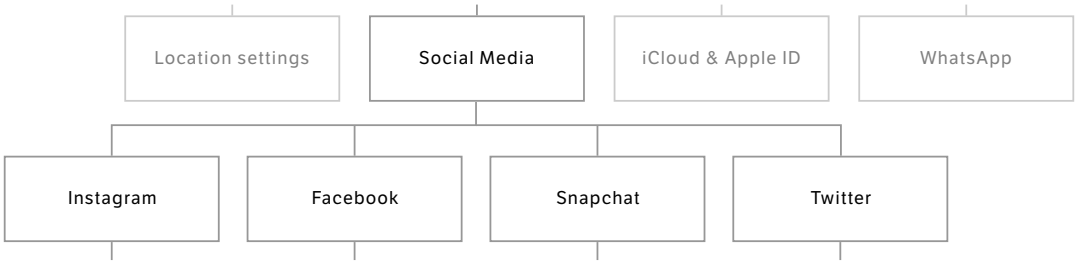

Fig. 21. Second-level *Social Media* menu

Each of the second-level menu items then offers third-level options that the user must select from, such as 1) reviewing users logged into an account, 2) managing post privacy, 3) changing passwords, 4) *blocking* another user, and 5) managing location permissions, depending on the particular features offered by each social media platform. For example, only Facebook allows users to review all devices that are logged into an account, therefore, the Facebook submenu has specific options that are different from, for example, Instagram. All the third-level menu options lead directly to a single video each, with the complete list being:

- Review logged-in devices on Facebook (iPhone and Android);
- Review Facebook post privacy settings (iPhone and Android);
- Change a Facebook password (iPhone and Android);
- *Block* someone on Facebook (iPhone and Android);
- Facebook location settings (iPhone and Android);

- Review Instagram post privacy settings (iPhone and Android);
- Change an Instagram password (iPhone and Android);
- *Block* someone on Instagram (iPhone and Android);
- Instagram location settings (iPhone and Android);
- Review Snapchat post privacy settings (iPhone and Android);
- Change a Snapchat password (iPhone and Android);
- *Block* someone on Snapchat (iPhone and Android);
- Snapchat location settings (iPhone and Android);
- Review Twitter post privacy settings (iPhone and Android);
- Change a Twitter password (iPhone and Android);
- *Block* someone on Twitter (iPhone and Android);
- Twitter location settings (iPhone and Android).

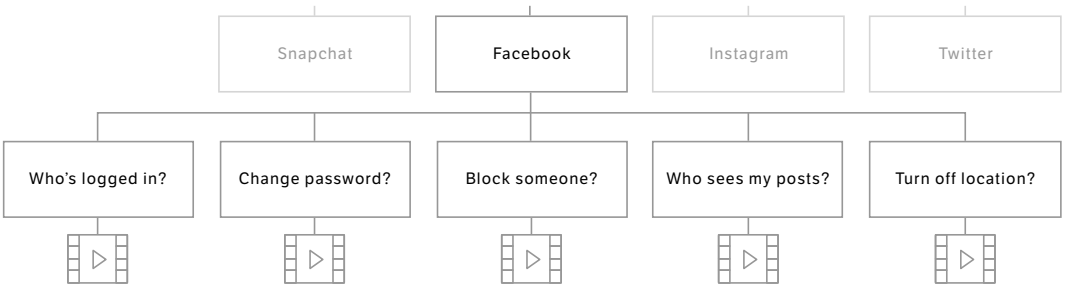

Fig. 22. Third-level Facebook menu

APPLE ID & ICLOUD

The *Apple ID & iCloud* menu item (Fig. 23) only appears within the iPhone journey and contains videos on 1) reviewing which devices are logged in to an Apple ID account, 2) changing an Apple ID password, 3) and managing location sharing within Apple's Family Sharing feature. This top-level menu item is only available on the iPhone journey, as Apple ID and iCloud are exclusive to the Apple ecosystem. Android does not offer a direct or commonly used equivalent, therefore, the Android journey has only 3 top-level menu items.

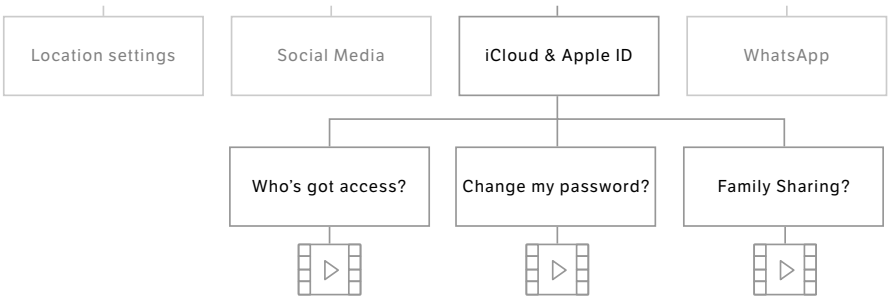

Fig. 23. Second-level Apple ID & iCloud menu

The complete list of videos in Apple ID & iCloud is:

- Review devices logged into an Apple ID account;
- Change and Apple ID password;
- Review location settings on Family Sharing.

WHATSAPP

Finally, the *WhatsApp* menu item contains all videos related to managing privacy on WhatsApp. Each of the second-level items seen in Fig. 24 leads directly to an instructional video. The *WhatsApp* menu item is available for both the iOS and Android journeys.

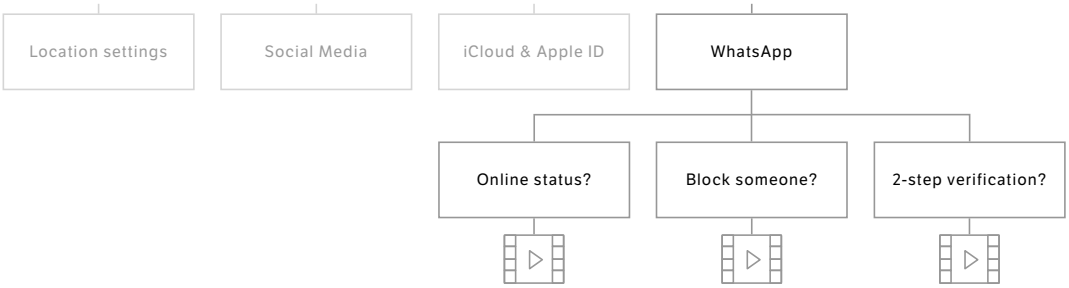

Fig. 24. Second-level *WhatsApp* menu

A complete list of WhatsApp videos is:

- *Block* someone on WhatsApp (iPhone and Android);
- WhatsApp location settings (iPhone and Android);
- Enable two-step verification on WhatsApp (iPhone and Android);
- Review online status settings on WhatsApp (iPhone and Android).

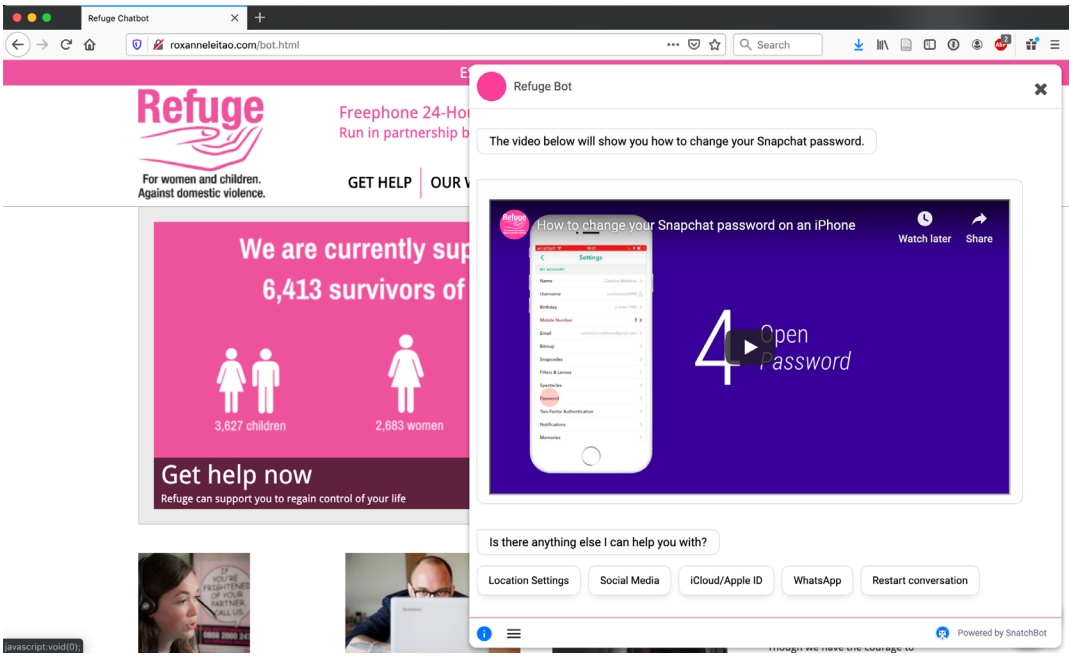

Fig. 25. *Refuge Bot* displaying the main menu after each video

Finally, after each video, the top-level menu is again displayed to users (Fig. 25). Initially, the bot had been designed to display contextual second-level menus after each video, related to the category of that particular section. For example, if a user had just watched a video on how to change an Instagram password, the second-level Instagram menu would be presented after the video. However, this structure was found to be inadequate to participants' mental models of the menu system during the co-evaluation sessions. Participants found the bot easier to use when the top-level menu was presented after each video, rather than second-level contextual menus (see Section 6.4 for further detail).

5.3.3 INSTRUCTIONAL ANIMATED VIDEOS

The videos all follow the same structure and layout. The layout displays a mobile device — iPhone or Samsung — on the left of the screen and textual instructions on the right (Fig. 26). The videos were recorded as screen captures on mobile devices and then placed within the mockup image of an iPhone or Samsung device. The textual instructions include location cues, such as "select the arrow at the top-left corner to go back", as well as references to shape (e.g., "cogwheel icon"), which are intended to assist users in finding the correct UI controls as easily as possible. Each instruction remains onscreen for a minimum of 10 seconds and is extended for tasks that are more time-consuming (e.g., typing in an email address). The timing of the instructions was evaluated and adjusted according to participants' needs during the co-evaluation.

Similarly, instructions were adjusted and refined throughout the evaluation, leading to more detailed descriptions of the UI controls and their onscreen positioning (Section 6.4).

Also, the videos include a visual indicator (Fig. 26) that highlights the correct onscreen UI control. The visual indicator "pulses" three times to attract users' attention, before disappearing. Initially, the indicators faded-in, remained onscreen for 2 seconds, then faded-out. However, in the initial phase of co-evaluation, participants did not notice the visual indicators (see Section 6.4). Therefore, the indicators were doubled in size and a "pulse" was added. The redesigned indicators proved to be more effective in capturing users' attention during subsequent co-evaluation sessions. Finally, all videos close with the following message:

> *If you have other tech-related queries, you can find more resources in the "Our Services" section of the website.*

5.4 TECHNICAL DEVELOPMENT

This section briefly describes the technical implementation of the chatbot, from the choice of a development platform to technical aspects of creating the videos.

5.4.1 DEVELOPMENT PLATFORM

The bot was created using a cloud-based developer platform called Snatchbot2. Developer platforms facilitate the creation of chatbots by simplifying the processes of sketching dialogue flows, providing machine learning capabilities, and API integrations, which allow for the more rapid creation of minimal viable products (MVPs). The Snatchbot platform also hosts chatbots developed using its platform and provides deployment functionality across web and instant messaging channels. In this context, Snatchbot was selected as the platform of choice to create the MVP for several reasons:

- Snatchbot is community-built and -maintained, as opposed to other prominent chatbot developed platforms such as Dialogflow (Google, 2019) and Watson Assistant (IBM, 2018), which are owned by Google and IBM respectively.
- Furthermore, contrary to Snatchbot, platforms such as Dialogflow and Watson Assistant do not provide a pricing plan for charities, nor are they free to use. Snatchbot is freeware and will, therefore, incur no building costs to the community partner;

2 https://snatchbot.me/

- Snatchbot hosts chatbots on its servers free-of-charge, eliminating hosting costs for the community partner.
- Snatchbot regularly updates and maintains its platform to ensure ongoing functioning with OS updates, minimising the need for ongoing technical maintenance for the community partner.

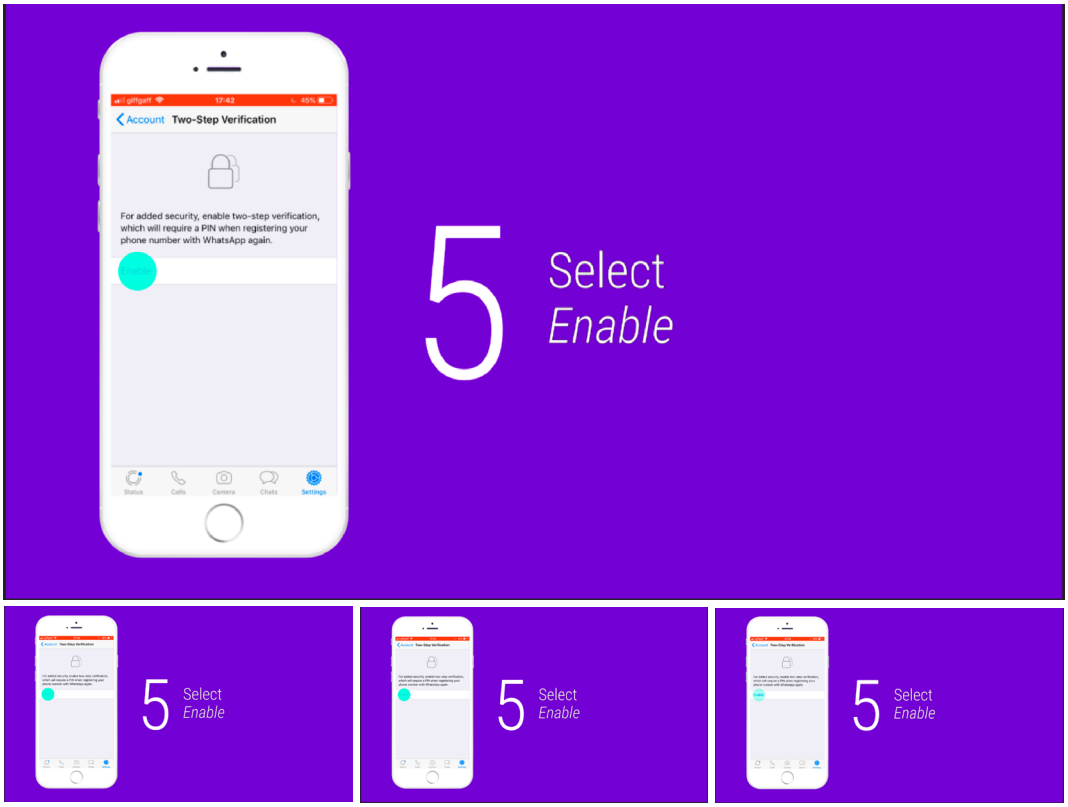

Fig. 26. Example video and onscreen UI controls indicator

Finally, it is important to note that further work carried out to improve the bot's accessibility may require that the bot be rebuilt without the use of a platform such as Snatchbot. Although Snatchbot facilitated the creation of a proof-of-concept and MVP, the nature of the platform does impose limitations on the structure and presentation of the bot, which could impact overall accessibility in certain ways. Namely, the structure of Snatchbot imposes constraints on what can be done to create custom keyboard navigation for screenreader users.

5.4.2 VIDEO CREATION

Videos were captured as screen recordings on an iPhone or an Android device. They were then imported into Adobe After Effects, which was the tool used to create all of the

animated videos. All user accounts (e.g, Facebook, Apple ID) seen in the videos were created for a fictional user called Caroline Mathews, to avoid divulging real account details online. Finally, the videos are hosted on Refuge's YouTube account, where the chatbot can access them for embedding.

5.4.3 OWNERSHIP, DEPLOYMENT, AND MAINTENANCE

As a designer, I performed all the technical development of the chatbot and maintained ownership of all accounts — Snatchbot and YouTube — during this period. Towards the end of the first development iteration, and prior to the co-evaluation, Refuge's main IT collaborator was granted access to the chatbot's backend. Access was granted in order to collaborate on transferring ownership of the chatbot to Refuge. At the time of writing, Refuge has full access to the Snatchbot and all videos hosted online. Similarly, all After Effects files and original screen capture videos have been transferred to Refuge. This effectively enables Refuge to maintain, modify, and update the bot as they see fit.

5.5 DISCUSSION & FUTURE WORK

This chapter has described the process of developing the artefact — *Refuge Bot* — that resulted from the codesign process with DA survivors and support workers. The following sections will now offer a discussion on 1) plans for the future development of *Refuge Bot*, followed by 2) matters of ownership, agency, and collaboration throughout the co-development of the chatbot.

5.5.1 COMMUNITY OWNERSHIP & FUTURE WORK

At the time of writing, Refuge has taken ownership of the chatbot and have launched it on their public website[3]. Given that Refuge is one of the largest UK charities providing support to victims of DA, the chatbot is now available and accessible to survivors all across the UK who may be seeking assistance and information from Refuge and online. It is this goal of reaching victims, no matter where they are, that drives Refuge's plans to continue developing the chatbot. Refuge intend to extend the chatbot in a number of ways, to improve its accessibility for a wider range of victims/survivors. Initial plans for improved accessibility include, for example:

- translating the bot and videos into other languages beyond English;
- adding voice-over to the videos for users with low vision.

3 https://www.refuge.org.uk/

In order to do so, Refuge intends to secure funding that will enable them to collaborate with the technical partners necessary to implement these accessibility features. As in many participatory design projects, once the research ends and the researcher leaves, a gap in technical knowledge is created (Clement and Besselaar, 1993; Kensing and Blomberg, 1998; DiSalvo and Pipek, 2013; Taylor *et al.,* 2013). Such gaps in technical know-how can mean that the community either needs to upskill their members or collaborate with new partners to continue the work that was initiated by the researcher. In Refuge's case, they have planned to apply for the funding necessary to create collaborations with new technical partners, to continue the accessibility work.

Refuge's plans for improving the first iteration of the chatbot demonstrate a sense of ownership and desire to continue the collaborative work that began with this PhD. The exact form that such future work will adopt is still unclear, however, it is important to note that during the collaboration, one of Refuge's *Tech Champions*[4] shadowed me with the aim of developing the facilitation skills necessary to the co-creation and co-evaluation (Chapter 6). In fact, after a few sessions, the *Tech Champion* began to actively participate in facilitation and eventually took the lead on two sessions with survivors who did not speak English (see Section 6.2.1). Refuge's aim in developing codesign facilitation skills in-house was performed with the knowledge that the PhD would come to an end and that it therefore needed to seize the collaboration as an opportunity for knowledge exchange and upskill its *Tech Champions.* Such an exchange of skills and knowledge between designers/researchers and community participants has long been one of the goals of participatory design (Robertson and Simonsen, 2012), as it facilitates the continuation of codesign processes once the designer/researcher leaves the community. This intentional collaboration in skill-sharing leads us onto the discussion below regarding participation, ownership, and agency within the process of co-developing the chatbot.

5.5.2 OWNERSHIP, AGENCY, AND COLLABORATION

Despite Refuge's current ownership of the Bot, it could be argued that survivors were not involved in the co-development of the chatbot to the same extent as Refuge staff. As seen in this chapter, the main actors involved in shaping the final concept were Refuge staff and me, as a designer, despite this shaping process being informed by 1) findings from the workshops with survivors (Section 4.3), as well as 2) the interviews and focus groups with survivors aimed as discussing the chatbot concept (Section 5.1 and Appendix E).

4 *Tech Champions* are Refuge staff that have been trained to support and respond to high level technology-facilitated domestic abuse cases.

The closer collaboration with support workers took place mainly due to the complex nature of recruiting survivors of IPA who could be involved in co-developing the *Bot.* The co-development phase involved multiple sessions in rapid succession of one another, required continuity of participants, and overall project knowledge between sessions. Limitations on my capacity to maintain the high degrees of collaboration necessary to a co-development phase happened for several reasons. Firstly, the process of recruiting survivors is a lengthy one, which throughout this PhD often took as long as 6 months for the interviews (Chapter 3) and a further 8 months for the workshops (Chapter 4). Secondly, the complex life situations in which survivors are placed when rebuilding their lives, post-separation from abusers, often means that survivors do not have the time, nor the availability, to participate in multiple consecutive codesign sessions. In fact, it could be argued that the time investment necessary to fully participate in codesign may not always be in survivors' best interest, as they have many more life-impacting situations (e.g., housing, finances, childcare) in which to invest time and effort. In this context, the feasibility of recruiting survivors for multiple iterative concept co-development sessions was severely limited. Albeit, survivors were consulted by Refuge on the concept of the chatbot and contributed with important feedback and ideas that shaped the chatbot (Section 5.1). Survivors were also fully involved in the co-evaluation of the Bot and iterative refinements that took place as a consequence of the evaluation (see Chapter 6).

Extents and forms of participation in codesign necessarily vary according to context, community and non-community participants, timeframes, and costs of participation, amongst other factors (Byrne and Alexander, 2006; Robertson and Wagner, 2013). In an attempt to clarify extents of participation in codesign, Mattelmäki and Visser (2011, p. 2) draw attention to the fact that participants can assume many roles throughout the collaborative process, such as being an *"information provider, a creative mind, an evaluator of new ideas, etc."* and that those roles are not solely restricted to solution ideation. In this context, and although participants were not extensively involved in shaping the concept of the chatbot, they were central in the processes of understanding the problem space (Chapter 3), shaping the design brief (Chapter 4), and evaluating the chatbot (Chapter 6) through the interviews, codesign workshops, and co-evaluation sessions respectively.

In fact, throughout this work, stakeholder groups have been involved to varying extents at different stages of the process. During the interviews, I mainly collaborated with survivors and frontline staff from DVIP, VS, and Domestic Shelters. For the workshops, the codesign mainly unfolded alongside survivors and staff from Changing Pathways,

DVIP, and Respect. During the co-development of the chatbot, it was mainly Refuge management and frontline staff that shaped the evolution of the concept, whilst direct collaboration with survivors was less intensive. The nature of the interviews and workshops, which could be spaced apart in time and did not require continuity of people or content from one session to the next, rendered them more suitable to the participation needs of survivors. On the other hand, as previously mentioned, the rapid and iterative nature of co-developing a concept and the ensuing technical implementation meant that codesign sessions took place in rapid succession of one another (e.g., weekly) and required many of the same participants, as well as continuity in participants' knowledge of the content being discussed, from one session to the next. Such levels of required participation meant that Refuge and I were unable to recruit survivors who were able to engage. For these reasons, the focus and interviews with 48 survivors were arranged and conducted by Refuge outside of the co-development sessions. What is more, to run the interviews and focus groups within a timeframe suitable to the co-development, Refuge — rather than I — led the sessions, limiting the need to go through formal university recruitment processes. In this manner, Refuge and I were able to bring survivors' voices into the co-development whilst managing constrained timelines and resources inherent to the PhD research.

In fact, a necessary shift in the dynamics of participation led to a broadening of the chatbot's envisioned usage scenarios from a focus purely on survivors to a new group: frontline staff. As seen in the workshops and interviews, frontline staff are often not confident in their own digital privacy literacy and capabilities. Support workers tend to feel that they do not know enough about digital privacy management to effectively support victims, without the concern that they may make the situation worse by providing incomplete or inaccurate advice. In this context, throughout the co-development of the chatbot, a new usage scenario emerged. One in which support workers use the chatbot alongside survivors during instructional workshops on digital privacy management. Digital privacy workshops with survivors are already being run, in shelters, by Refuge's *Tech Champions.* However, these workshops currently rely on printed handouts of written instructions. The *Tech Champions* felt that the visual step-by-step nature of the chatbot videos makes the content easier to comprehend and engage with. Therefore, the *Tech Champions* intend to use the chatbot and videos as replacements for the printed instructional materials they had been previously using. As Le Dantec (2012) argues, based on his experience of using technology within a shelter for homeless mothers, technology can play a significant role in shaping the relationship between service

providers and service users. In the case of this PhD, an unintended consequence of this work is the change in format of the *Tech Champions*' digital privacy workshops, which will now be supported by the chatbot and instructional videos.

As highlighted by Le Dantec and Fox (2015), design with communities extends the responsibilities of the designer beyond those of structured inquiry, into the spaces of managing participation and collaboration by developing relationships with communities, demonstrating ongoing commitments to the community, and overcoming personal and institutional barriers to community-based design research. A significant portion of my time, on this PhD, was invested in building relationships with the community through volunteering (demonstrating ongoing commitment), as well as developing the research with community members and attempting to overcome barriers such as participant recruitment and staff time constraints. The codesign process has thus been a highly flexible and adaptable one, where initial plans for participation at different stages of the design process have been adapted to the context and situations that were taking place then. "Then" as in the real moment of the design activities in the real world, within participants' daily lives and responsibilities (Le Dantec and Fox, 2015). The emergence of a novel *usage scenario* which involves frontline staff and survivors using the chatbot in collaborative sessions highlights the dynamic nature of the codesign process. Had the circumstances and barriers of participation, stakeholder groups, or even myself as a researcher been different, the output of the codesign process would have likely been different too.

For instance, through the project and before the co-development phase of the chatbot began, one of the charities I had been collaborating with was bought by a larger non-specialised charity. A restructuring took place and many frontline staff were made redundant, which had the effect of completely altering the composition, motivation, and goals of the remaining staff. Whilst their engagement with me, in both my capacities as a volunteer and an independent researcher, had begun as an enthusiastic endeavour that was seen as valuable to all of those involved, once the charity had been bought out, staff no longer had the time nor the motivation to progress the codesign further. In another example, one other charity that had taken part in the initial phases of this work underwent continuous waves of restructuring to reduce operational costs. In practice, this meant that my contacts and volunteer activity line-manager were replaced several times in the space of 12 months. Understandably, not all staff were equally optimistic about the research and the codesign, which effectively led the collaboration to come to a progressive end after around 18 months of work.

The significant operational and financial constraints inflicted upon charities, especially domestic abuse charities, over the last decade have been documented by the media (Oppenheim, 2018; Dudman, 2019). The effects of austerity have meant that, all over the UK, refuges are being closed and victims are being denied support due to a lack of refuge space. Understandably, support workers often find that they do not have the capacity to participate in activities beyond essential service delivery, which has been evident throughout different stages of this work. Due to these factors, building relationships with key individuals within the charities was a process full of starts and stops, lulls and highs, which impacted my ability to involve staff and survivors in an ongoing, iterative, and steady process of codesign in this co-development phase of the work. Given that recruiting survivors depends on support workers' engagement and ability to recruit, if staff do not have time then the researcher is unable to reach survivors who could be involved in the codesign.

Nonetheless, I sought to nurture existing relationships with DA charities, as well as create new ones throughout the PhD, adapting to the changes in circumstances that are inevitable with the progression of time and within such a complex problem-space. The process of infrastructuring this work by continually nurturing existing relationships and building news ones to sustain a community of participants was ongoing throughout the PhD and aligns with existing analysis of PD projects and their processes (Björgvinsson, Ehn and Hillgren, 2012; Dantec and DiSalvo, 2013). Support workers and survivors effectively collaborated within the codesign process, throughout the discovery, problems definition, development, and as seen in the next chapter, evaluation phases, even if survivors' involvement was less intense during the co-development of the chatbot.

Notwithstanding, participants involved in the co-development stated that the chatbot will be beneficial to victims/survivors and support workers in several ways:

- the chatbot is remotely accessible online and, therefore, available to victims/survivors beyond those engaged with formal support services;
- victims/survivors can access information anonymously using the chatbot;
- due to its automated nature, the chatbot is always available;
- the instructional animated videos may be better suited to delivering digital privacy management content than instructions delivered by a human over a phone-based helpline.

In this discussion, I have sought to highlight aspects of collaboration during the co-development phase, with the aim of making it clear to the reader why the project progressed in the manner that it did. Furthermore, by highlighting such processes and difficulties inherent to codesign with survivors of IPA, this research aims to contribute to an ongoing body of work discussing the nature of conducting participatory design projects within sensitive topic areas (Southern *et al.,* 2014; Le Dantec and Fox, 2015; Mulvale *et al.,* 2016). A more in-depth discussion on the dynamics of participation and specific contributions to the field of codesign within sensitive topics can be found in Chapter 7, where the broader context of participation throughout this work is considered.

5.6 CONCLUSION

This chapter described the co-development of a chatbot alongside the community partner Refuge and DA survivors. In addition to outlining the design and technical development of *Refuge Bot,* I also introduced a discussion on the dynamics of participation for different participant groups during the co-development. This work has contributed, alongside existing literature (Southern *et al.,* 2014; Le Dantec and Fox, 2015; Mulvale *et al.,* 2016) arguing for the flexible and adaptable nature of codesign and participation, especially within sensitive topic areas, which often requires reflexivity and adaptation as projects progress. This chapter contributes to the broader aims of the PhD through:

- a discussion on the participants and their roles during the co-development, which contributes to existing discourse on roles and dynamics of participation within codesign within sensitive topic areas (Southern *et al.,* 2014; Le Dantec and Fox, 2015; Mulvale *et al.,* 2016);
- a description of the co-development process of an MVP alongside support workers and survivors.

6

CHATBOT CO-EVALUATION

This chapter describes the process of co-evaluating *Refuge Bot* alongside support workers and survivors of intimate partner abuse (IPA). The co-evaluation took place between July and September 2019 before the bot was launched on Refuge's website. Recent usage statistics from the 05/09/2020 to the 27/11/2020 (90 days) show that 971 people have interacted with the chatbot over this period. Of the top-level menu items, Location Settings was selected 277 times, WhatsApp 269 times, Social Media 185 times, and iCloud & Apple ID 52 times. From the 09/01/2020 to the 31/03/2020 (90 days), before the COVID-19 social distancing measures, 164 individual people used the chatbot.

6.1 CO-EVALUATION SESSIONS WITH SURVIVORS AND SUPPORT WORKERS

The aims of the co-evaluation alongside survivors and support workers were to:

- gather feedback regarding the chatbot and its appropriateness to the problem it is intended to address;
- assess the effectiveness of the content and its format for communicating and conveying digital privacy management information;
- evaluate the feasibility and acceptability of a fully automated conversational agent for providing digital privacy information and advice to survivors of DA;
- iteratively implement modifications based on participants' feedback;
- assess and improve the overall user-experience of the chatbot.

The co-evaluation involved several activities with different focusses and participant groups. The primary activity consisted of one-to-one co-evaluation sessions each of

which involved the designer/researcher, a Refuge *Tech Champion,* and an IPA survivor. Secondary activities included 1) gathering feedback via email from Refuge support workers across the UK, 2) informal feedback from support workers during our visits to Refuge shelters, and 3) a technical cross-browser and cross-device evaluation of the chatbot alongside Refuge's IT team.

The co-evaluation sessions and design modifications were iterative in nature. Between sessions, the chatbot was modified to address participants' feedback before being presented to another group of participants. In this manner, issues raised by one group of survivors could be addressed and the effectiveness of the modifications evaluated by the next group of participants. Similarly, feedback received via email was also addressed in cases where it matched the feedback being gathered in the co-evaluation sessions. Due to the higher degree of Refuge staff involvement in the co-development of the chatbot (Chapter 5), a stricter focus was placed on survivors' contributions during the co-evaluation, thereby ensuring that actioned feedback had its origin in survivors' contributions and requirements. Hence, more weight was given to the co-evaluation feedback from survivors and email feedback was actioned when it aligned with survivor feedback. Finally, while the co-evaluation was ongoing, regular meetings with Refuge were scheduled to review feedback and discuss modifications that required consensus between stakeholders. Examples of such modifications were those that provoked a shift in project timelines.

The sections below provide further detail on the procedure for all of the activities that took place as part of a co-evaluation process.

6.2 PROCEDURE

To contextualise the co-evaluation findings, this section offers a description of the process and its procedures. Firstly, the face-to-face co-evaluation sessions with survivors are described, followed by the procedure for receiving email feedback from Refuge support workers, and finally, the technical cross-device testing of the chatbot.

6.2.1 PROCEDURE: CO-EVALUATION SESSIONS

All co-evaluation iterations took place between the August 20th 2019 and September 25th 2019, with varying intervals of time between them. A few iterations took place one day after the other, while others were spaced apart by one to two weeks, depending

on participant, shelter, or outreach service[1] availability. Each iteration included three to nine individual co-evaluation sessions with participants.

PARTICIPANTS

All participants identified as female and their real names have been replaced with pseudonyms. 15 were in a Refuge shelter at the time of participation, 4 were accessing a Refuge outreach service, and 9 participants were Refuge staff[2]. Throughout the remainder of this chapter, the terms *refuge* and *shelter* are used interchangeably to refer to emergency accommodation provided to victims of DA who have fled their homes.

INFORMED CONSENT

Participants were briefed and asked whether they wished to take part in the co-evaluation prior to my visit. Participants were briefed by a Refuge member of staff who had been sent the Participant Information Sheet (Appendix G) and Consent Forms (Appendix H) in advance. Therefore, all participants had already expressed interest in taking part before any interaction with me.

A Refuge support worker — *Tech Champion* — was present during all co-evaluation sessions. The *Tech Champion* introduced me and briefly explained the aims of the co-evaluation. I then discussed the activity in more detail and answered any questions that participants may have had. Participants were given time to read the Participant Information Sheet and Consent Form. Whenever participants did not understand the Information Sheet or Consent Form, I verbally explained the study and participation. Consent was obtained before all sessions. Once participants had consented to take part and all of their questions had been answered, I performed a short demonstration of the chatbot. All sessions were performed on a one-to-one basis, however, in some cases, the initial briefing took place in a group setting at the end of one of the *Tech Champion's* digital privacy workshops.

One participant did not wish to take part as she was not able to understand the Information Sheet nor my explanation of the study. The participant did not understand English in written or oral form. One other participant was able to take part in the study in her native language — Punjabi — as the Refuge *Tech Champion* was able to translate all the oral content and the participant was able to read the English content.

1 Refuge refers to services that are not shelters and are open to supporting victims living in the community as *outreach services.*
2 Refuge staff took part in their professional capacities even though a high percentage of staff are DA survivors themselves.

During some of the sessions, either the *Tech Champion* or I provided childcare assistance to participants. Childcare was not available at the shelters or outreach locations during the time of the co-evaluation sessions. Therefore, a few of the sessions were performed whilst either the participant or I were taking care of participants' children. The format of the sessions had to be adapted, in the moment, to participants' childcare needs in order to include childcare breaks and entertaining children. The sessions included breaks whenever participants needed them, as well as the repetition of questions and restarting of scenarios as necessary.

LOCATION

Four of the co-evaluation sessions took part in Refuge shelters across London. More specific geographic details are not disclosed to protect the shelters' location. The session with survivors who were not living in a shelter was conducted at one of Refuge's outreach services also in London. The evaluation session with support workers was conducted at Refuge's London headquarters with support workers travelling from across the UK for the day.

SETUP

The sessions with survivors were conducted in a communal space within each of the shelters or outreach service, such as the kitchen, living room, or waiting area. Women are generally given a private bedroom within a shelter and all other living spaces are communal. Women's bedrooms are their personal space and therefore, it would not be appropriate for me to request that the sessions take place in their private quarters. Hence, the shelter sessions all took place in communal spaces where children were often playing and other residents socialising. During most of the sessions, childcare was not available. Therefore, the support worker and I often engaged in childcare to give participants the time and space needed to take part. Even so, in most cases, women were interrupted by childcare duties during the session, requiring them to take breaks and then return once the children had been attended to.

During the evaluation, participants used the chatbot to complete the four scenarios listed in Table 2, on either an iPhone or Android device. All scenarios were information finding scenarios focussed on privacy settings that may be necessary to DA survivors, as informed by the interviews, codesign workshops, and my tacit knowledge of technology-facilitated IPA gained through working alongside survivors.

Participants were asked to use the chatbot on an iPad and follow the video instructions using either an iPhone or Android phone, according to the operating system (OS) they were most familiar with. All devices were provided for participants.

DATA CAPTURE

For the co-evaluation sessions, audio and iPad screen recordings were captured. I also took extensive notes and discussed these with the *Tech Champion* after each of the sessions.

Scenario	**Operating System (OS)**
1. Change your Snapchat password	iPhone & Android
2. *Block* another Instagram user	iPhone & Android
3. Stop a specific person from seeing your Facebook posts without *blocking* them	iPhone & Android
4. Disable Snapchat's use of location data	Android
5. Disable Apple Family Sharing's use of location data	iPhone

Table 2. Co-evaluation scenarios according to OS.

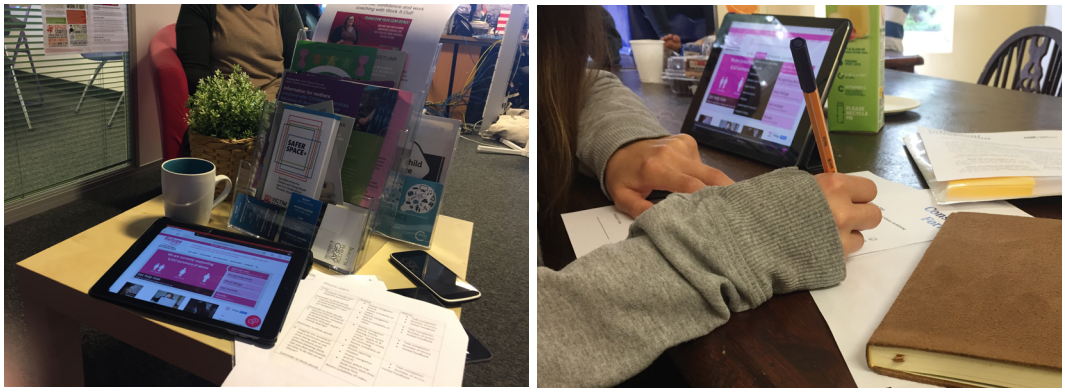

Fig. 27. Co-evaluation images (taken with participants' consent)

6.2.2 PROCEDURE: EMAIL FEEDBACK

Support workers across Refuge were sent a request via email to use the chatbot and give feedback. Eleven participants gave feedback via email. The email requesting feedback was sent out on August 30th 2019 and all feedback was received between September 3rd 2019 and September 6th 2019. Feedback was sent to Refuge's Director of Operations and then forwarded to me.

The email requesting feedback asked participants to use the chatbot and then answer the following questions:

- *What are your general impressions of the chatbot?*
- *How easy/difficult was it to use the chatbot for the first time?*
- *Did you watch any of the videos?*
    - *What are your thoughts on the video/s you watched?*
    - *How did you find the experience of following the instructions in the video/s?*
- *In what contexts do you think the chatbot could be used by victims and survivors? (If any at all)*
- *Would the chatbot be useful to you in your work with clients? If yes, in what ways?*
- *Is there anything you think should be changed/improved?*
- *Was there anything that seemed to not be working properly? Can you describe it? Or send a screenshot of the issue?*
- *Do you have any other thoughts you want to share that we haven't asked about?*

6.2.3 PROCEDURE: CROSS-PLATFORM TESTING

Throughout the development process, the chatbot was tested and optimised to function across desktop and mobile devices, as well as on recent versions of Chrome, Safari, and Firefox. To perform the testing and optimisations, I relied on 1) emulators for iOS devices, 2) an iPhone 6, 3) an iPad 2 Air, 4) a Nokia Android device, and a 5) Samsung Galaxy Tab A.

Ongoing testing aimed to evaluate and optimise the following aspects of the chatbot:

1. Window size for large screens (e.g., laptops), medium screens (e.g., tablets), and small screens (e.g., mobile phones);
2. Embedded video dimensions on large and medium screens;
3. Fullscreen video functionality on small screens;
4. Font sizes across all screen sizes;
5. Button sizes and behaviour across all screen sizes.

In addition, once the chatbot was ready for its final testing phase, I collaborated with Refuge's IT team on a full review of its cross-device functionality (see Section 6.5 for summarised findings and Appendix F for a full report).

6.3 ANALYSIS

Screen and audio recordings from the co-evaluation sessions were reviewed and coded. Although the sessions were not transcribed in full, qualitative feedback was transcribed, coded, and themed (Charmaz, 2014; Saldana, 2015). Feedback received via email was coded alongside the qualitative co-evaluation data. Transcripts were coded using a combination of descriptive and *in-vivo* coding (Charmaz, 2014; Saldana, 2015). The codes related to:

- participants' qualitative feedback and opinions regarding the chatbot;
- whether or not a scenario had been completed;
- barriers faced by participants during the scenarios;
- success factors during the scenarios;
- other contextual factors influencing the co-evaluation (e.g., childcare).

Codes were then grouped into overarching *observations.* These observations are reported on in the sections that follow. Each observation is paired with the design changes that were made as a result of that observation. The design responses are modifications intended to address observed issues and were implemented between co-evaluation iterations. The sections that follow are organised according to the order in which the co-evaluation sessions took place.

6.4 FINDINGS

Findings are presented for each of the co-evaluation iterations and are organised in chronological order. In this way, it is clear which design modifications were implemented from one iteration to the next and the effect they had on the co-evaluation findings.

6.4.1 CO-EVALUATION SESSIONS: 1ST ITERATION

Four participants took part in the 1st iteration of the co-evaluation. All participants were female. Participants took part in 1) a collective brief and then 2) used the chatbot individually to complete four scenarios, followed by 3) a discussion with *Tech Champion* and me on their opinions and thoughts regarding the chatbot. Table 3 provides an overview of the four scenarios and each participants' experience of either finding the intended information (Y) or not finding it (N), as well as whether the video instructions were clear (Y) or not (N). Below is a thematic grouping of the observations from this initial co-evaluation session, as well as the design modifications that were proposed as a response to participants' feedback.

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Aria	Y	N	Y	N	Y	Y	Y	Y	N/A	N/A
Calla	N	N	Y	Y	Y	Y	N/A	N/A	N	N
Farah	Y	Y	Y	Y	Y	Y	N/A	N/A	N	N
Hester	N	Y	N	Y	N	Y	N	N	N/A	N/A

Table 3. Did participants find the information they were looking for? And were the video instructions clear?

Observation 1: It was confusing for participants when the chatbot suggested other related videos below a given video and above the sub-menu (Fig. 28).

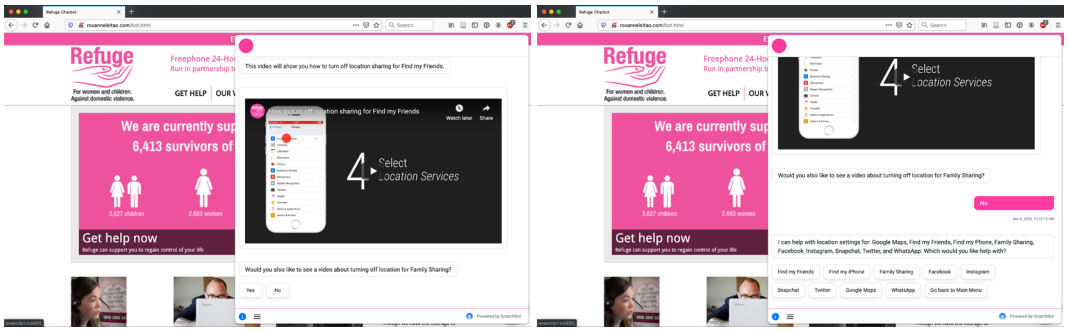

Fig. 28. Chatbot displaying related videos

Design response: Suggested videos were removed for the next version of testing and the sub-menu was maintained..

Observation 2: Videos progressed too quickly for participants to read the instructions and carry them out on a mobile device. Some participants were able to pause and rewind the videos, although this added time and effort to the task.

Design response: Increase the onscreen duration of each instruction to avoid the need for pausing/rewinding so often.

Observation 3: Participants were not able to make the videos fullscreen.

Design response: Include a textual explanation on how to make the videos fullscreen in case it is necessary. Increase the size of the embedded videos to avoid having to make the videos fullscreen.

Observation 4: When asked to find the video for location settings on Family Sharing, some participants selected the Location Settings menu option. The video was only listed under the Apple ID/iCloud menu item and, therefore, did not match participants' mental model of where the video should be.

Design response: Include all videos related to location settings under Location Settings, even if this means that some videos are accessible via more than one route.

Observation 5: The interval between consecutive chatbot messages was too long (10 seconds). Participants were able to read each message far more quickly than the interval time, becoming visibly frustrated by having to wait.

Design response: Reduce time interval between chatbot messages.

Observation 6: When the chabot asked "Do you need help with anything else on [submenu section]?" and participants wanted to navigate to another submenu, they did not notice the option of "Go back to Main Menu" as a way to navigate back to the main menu (Fig. 29).

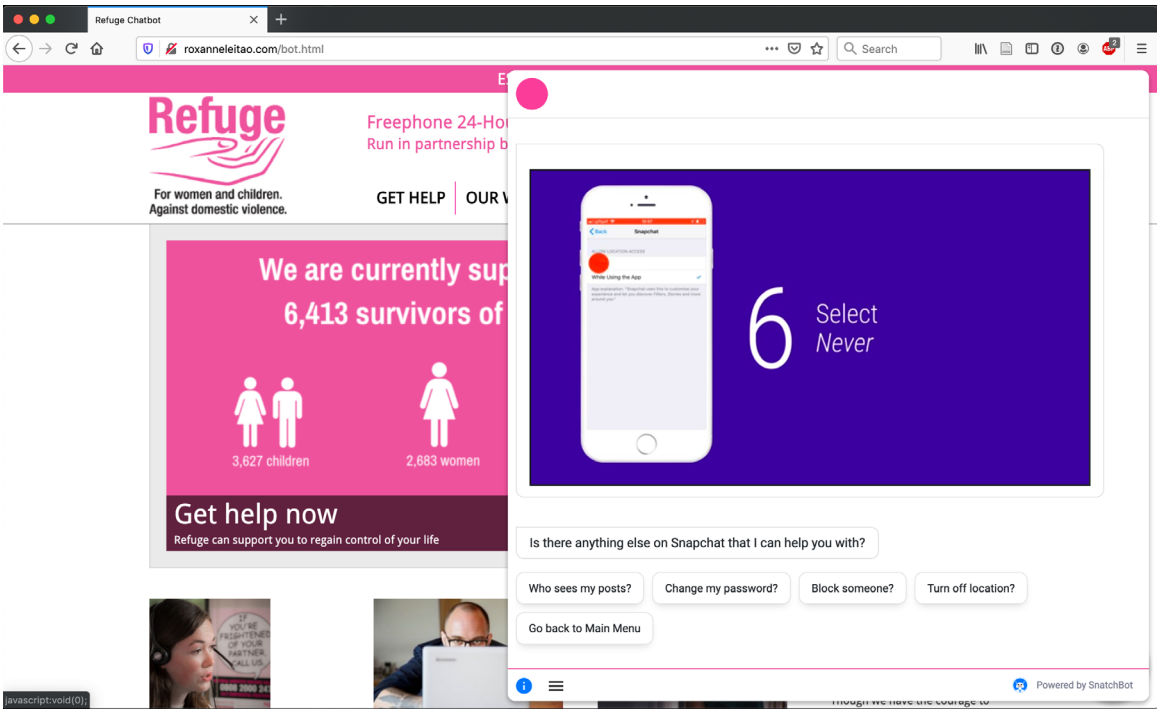

Fig. 29. Sub-menus displayed after each video (pre-redesign).

Design Response: Include the main menu at the bottom of the chat, rather than contextual sub-menus.

Observation 7: Overall, participants were positive about the instructional character of the videos, in which steps are textually described and supported by graphic representations, as observed by Aria.

> *Aria: I think it cannot be more simple than they already are — the videos — it's like step-by-step how to get there, what to do, it doesn't need more.*

Observation 8: Participants expressed the need for the chatbot to include videos for location sharing settings on Google Maps, in addition to the location videos that it already includes.

Design response: Create and include a location settings video for Google Maps on Android and iPhone.

6.4.2 CO-EVALUATION SESSIONS: 2ND ITERATION

As a response to the first iteration, a few changes were made to the chatbot before the second set of co-evaluation sessions, namely:

- All videos related to location settings were also included under the *Location Settings* menu item, as per Observation 4;
- The waiting times between consecutive chatbot messages were reduced, as per Observation 5;
- The main menu was presented to participants after each video, instead of the sub-menu related to the category they were currently within. The modification was made due to Observation 6, in the previous iteration, that the relationship between the main menu and contextual submenus did not match participants' mental model of how the content was organised.

The duration of the video instructions (Observation 2) was not modified, given the short time frame between iterations, which did not allow for sufficient time to amend the videos. Similarly, the size of the embedded videos (Observation 3) was not modified for this iteration due to a lack of sufficient time to solve a technically challenging issue. The underlying platform — SnatchBot — was undergoing significant technical maintenance at the time and the custom CSS functionality had been temporarily disabled, making it impossible to alter the size of the embedded videos.

Four survivors took part in the second co-evaluation iteration. All participants identified as female and were currently living in one of Refuge's shelters. Table 4 provides an overview of each scenario in this session.

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Ivana	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	N
Jeralyn	Y	Y	Y	Y	X*	Y	N/A	N/A	Y	N
Marisole	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	N
Quinn	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y

Table 4. Did participants find the information they were looking for? And were the video instructions clear?
*X = WiFi temporarily unavailable

In the second co-evaluation session, although participants were able to complete all the scenarios (Table 4), issues with the overall user-experience of the chatbot were still observed. Observations and design responses from this iteration are detailed below.

Observation 1: The new menu, rather than contextual sub-menus, displayed after each video was effective. Participants were able to navigate between sections and subsections more easily. I hypothesised that this alteration served participants in two ways: 1) it removed the complexity of creating a mental model of the main menu and submenus, and 2) it replicated the visual cue of the three main menu items that participants had already observed in their initial interaction with the chatbot (Fig. 30).

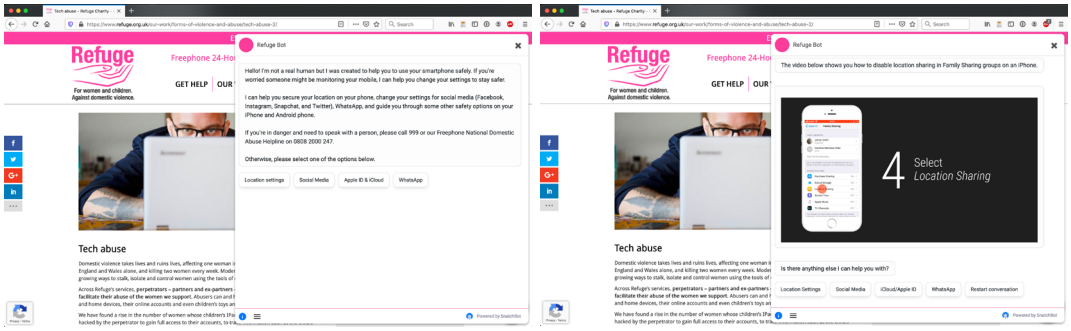

Fig. 30. The redesigned menu system.

Observation 2: Some participants attempted to type questions into the text-input box, even though it was greyed out (Fig. 31).

Design response: Remove the text-input box, as the chatbot does not support this type of interaction.

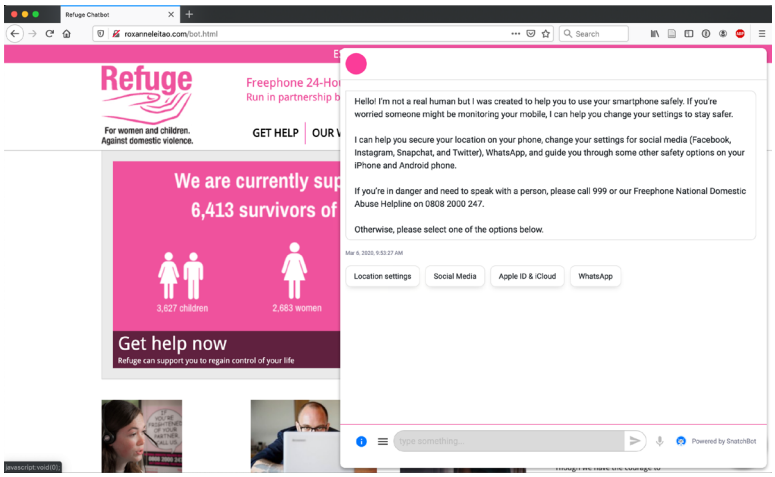

Fig. 31. Greyed-out text-input box

Observation 3: As in the first iteration, the videos progressed too rapidly for participants to read the instructions and carry them out on a mobile device. Participants were able to pause and rewind the videos as necessary, although, two participants only did so once I had suggested it.

Design response: Increase the onscreen duration of each instruction to reduce the need for pausing and rewinding.

Observation 4: For two of the participants, the chatbot timed out during longer videos and restarted itself.

Design response: Increase the time it takes for the chatbot to automatically reset itself.

Observation 5: As in the first iteration, participants seemed to prefer watching the video inside the chatbot window rather than navigating away to YouTube. However, fullscreen cannot be enabled from within the chatbot window.

Design response: Enlarge the videos embedded in the chatbot to avoid participants having to open the fullscreen videos on YouTube.

Observation 6: The notice on the Family Sharing location settings video, regarding notifications being sent to the primary family account owner (Fig 3), did not remain onscreen long enough for participants to read it in full.

Design response: Expand the duration of the notices, for all videos containing similar alerts.

Observation 7: None of the participants were able to complete all the instructions in the Family Sharing location video. The video includes disabling Family Sharing features beyond location sharing, such as purchase sharing, which unnecessarily increased the number of instructions and complexity of the task.

Design response: Focus the video solely on disabling location sharing. Other Family Sharing features are not as relevant to survivors and significantly impact the effectiveness of the video in addressing their main concern, which is location sharing.

Observation 8: Overall, participants expressed a positive opinion on the step-by-step character of the videos. As observed by Marisole, participants felt that the instructions were straightforward and easy-to-follow.

Marisole: [Unprompted, after completing the first video] It's quite clear and step-by-step. Also, like here [the text], it's short informations, and straight informations, it's good.

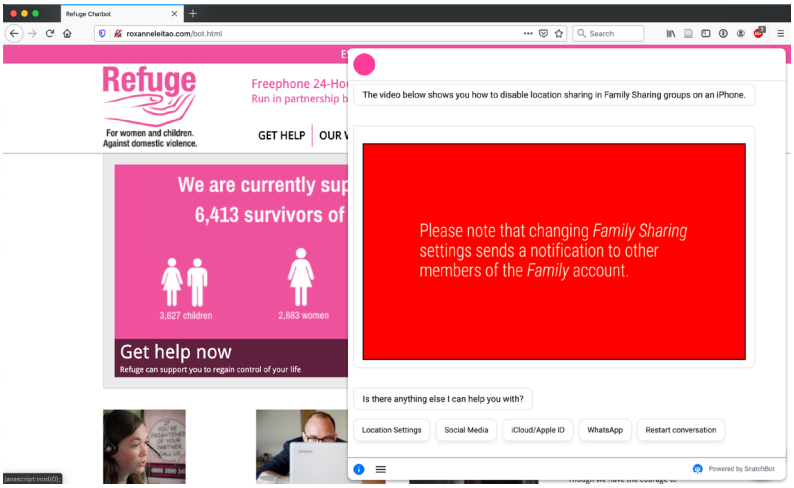

Fig. 32. *Family Sharing* location settings notice/warning.

6.4.3 CO-EVALUATION SESSIONS: THIRD ITERATION

No alterations to the chatbot were performed between the second and third co-evaluation iterations, as they took place one day after the other. Unlike in the previous iterations, participants in the third iteration were survivors of domestic abuse who were not living in a shelter. Participants had travelled to a Refuge outreach service to access legal advice from a solicitor. Participants had been contacted over the phone, by a member of Refuge's staff, regarding the research and had agreed to take part either before or after their scheduled consultation.

The table below shows participants' responses to each of the scenarios. The table is followed by session observations and proposed design responses, which describe actions to be taken as a result of survivors' feedback.

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Radha	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	N
Shea	Y	Y	Y	Y	X*	X*	N/A	N/A	X*	X*
Sia	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	N
Talitha	Y	N	Y	N	Y	Y	N/A	N/A	Y	Y

Table 5. Did participants find the information they were looking for? And were the video instructions clear?
*X = WiFi temporarily unavailable

Observation 1: All participants had trouble locating the Family Sharing settings by following the instructions in the video.

Design response: Add more detail to textual instructions indicating where specific UI controls are located onscreen (e.g., "at the top edge of the screen").

Design response: Make the visual indicator that shows users where to tap on the screen larger (Fig 6), as suggested by Amara.

> *Only thing I'd say, you know in the video, the small little circle — you can't actually see it that clearly.* [Amara]

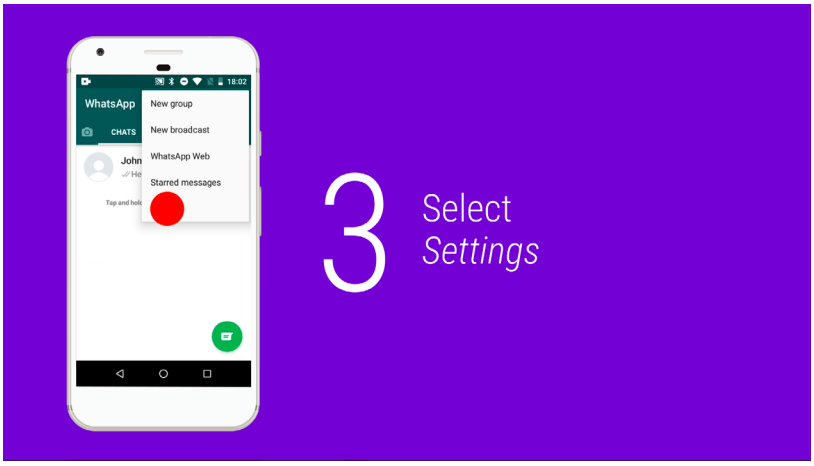

Fig. 33. Visual onscreen indicator made larger.

Observation 3: As in iterations one and two, the videos progressed too quickly for participants to read the instructions and carry them out on a mobile device. Three participants were able to pause and rewind the videos as necessary, however, this added to the time and effort necessary to follow the instructions in the videos, as highlighted by Sia.

> *Can I just say something about this? I have to keep pausing it to read what it was saying. I mean and that's fine as long as the person using it is comfortable with pausing but that might be something that could be fixable by making each step stay longer on the screen.* [Sia]

Design response: Increase the onscreen duration of each instruction to avoid the need for pausing/rewinding so often.

Observation 4: As in the previous sessions, two participants were unable to complete all the instructions in the Family Sharing location video. The video

includes disabling Family Sharing features beyond location sharing, such as purchase sharing, which unnecessarily increased the number of instructions and complexity of the video.

Design response: Focus the video solely on disabling location sharing. Other Family Sharing features are not as relevant to survivors and significantly impact the effectiveness of the video in addressing the main concern.

6.4.4 CO-EVALUATION SESSIONS: FOURTH ITERATION

All participants in iteration 4 were Refuge support workers, more specifically, service delivery managers. All delivery managers had been frontline support workers before becoming responsible for the operations of one or more of Refuge's shelters or outreach delivery services. Furthermore, as in previous stages of this work, many of the delivery managers were also DA survivors themselves, as highlighted by Refuge's Head of Operations.

Before the fourth co-evaluation iteration, a few changes were made to the chatbot:

- the *Family Sharing* video was simplified to focus solely on disabling location sharing;
- the duration of each video instruction was increased for all the Android videos. iPhone videos were not modified due to a lack of time before the fourth iteration.

As the iteration progressed, fewer observations and design changes were necessary, which indicated that the modifications were effective in addressing highlighted challenges. Only 2 observations and design responses were noted for this iteration. They are listed below.

The table below shows participants' responses to each of the scenarios. After the table, mine and *Tech Champion's* observations are listed alongside proposed design changes.

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Juliet	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y
Cecilia	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Florence	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Freya	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y
Amelia	Y	Y	Y	Y	Y	Y	Y	N	N/A	N/A
Caroline	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Hannah	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Holly	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Anne	Y	Y	Y	Y	Y	Y	Y	N	N/A	N/A

Table 6. Did participants find the information they were looking for? And were the video instructions clear?

Observation 1: Participants were better able to complete instructions with slower videos. Participants no longer mentioned that the Android videos were too fast.

Design response: Slow down remaining iOS videos to match the speed of the Android videos. Even though, as one participant expressed, it might be easier to pause and rewind the videos if participants' were using the chatbot on their own and in a different environment.

> *For me, I'm not technologically skilled, I keep having to go back. If I get stuck then I've gotta go back and I think, because this is an exercise, if I was at home and doing this I feel like I wouldn't be under that kind of pressure so I'd just keep going back, give it my own time. I think like, if I was at home, I'd still have the same problem because I didn't kinda fully understood, there was a part of it where it was saying about "the arrow" and I'm assuming that's the arrow because that's what I use when I'm going back, but if I was at home I'd mess about with it, so, eventually I'd get it right. But, um, yeah, I think that it's not really too fast. I think the speed is ok because I can go back, it explains what you're supposed to be doing but, yeah, I think for me I'd have to go back, look at this again, or I'd want to stop so that I could "right am I pressing the right thing? Am I looking at the right thing? Kind of thing".* [Anne]

Observation 2: A few participants did not realise that the first Snapchat video was a video and not a still image, this was due to the fact that the play button is a similar colour to the background colour on Snapchat videos.

Design response: Change background colour for Snapchat videos.

6.4.5 CO-EVALUATION SESSIONS: FIFTH ITERATION

No changes were made in advance of the fifth co-evaluation iteration, as it took place a day after the fourth iteration. Therefore, both observations and design responses listed below are the same as in the previous co-evaluation iteration.

As with iterations 1, 2, and 3, Iteration 5 was performed in collaboration with survivors of domestic abuse currently residing in a Refuge shelter.

Seven survivors took part in this iteration, however, four survivors' data has been excluded from this analysis. In the second shelter visited that day, participants did not wish to take part individually. Participants expressed the desire to take part as a group. However, the group dynamics and the fact that four young children were present without available childcare severely impacted our ability to structure the session. The support worker and I were unable to direct and maintain the conversation on topic whilst assisting with childcare. Furthermore, whilst the *Tech Champion* did attempt to translate the session for one of the survivors, this proved to be ineffective amongst the general levels of noise, background activity, and group dynamics. Finally, participants did not wish to use the chatbot themselves, out of fear of making "mistakes" in front of their peers, even though it was expressed that there were no "mistakes" that could be made. For these reasons, data from the second shelter has been excluded from this analysis.

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Yvette	Y	Y	Y	N	Y	Y	N/A	N/A	Y	N
Zara	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Amy	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y

Table 7. Did participants find the information they were looking for? And were the video instructions clear?

Observation 1: As with the fourth iteration, participants were better able to complete instructions with the slower videos. Participants no longer mentioned that the Android videos were too fast.

Design response: Slow down remaining iOS videos to match the speed of the Android videos.

Observation 2: A few participants did not realise that the first Snapchat video was a video and not a still image, this was because the play button is a similar colour to the background colour on the Snapchat videos.

Design response: Change background colour for Snapchat videos.

6.4.6 CO-EVALUATION SESSIONS: SIXTH ITERATION

For the final iteration of co-evaluation sessions, all participants were survivors living in one of Refuge's shelters.

Prior to the sixth co-evaluation iteration, one change was made to the chatbot:

- the remaining iOS videos were slowed down to match the same pace as the Android videos, as per Observation 1 in the previous iteration.

Participant/ Scenario	Snapchat password		*Block* Instagram user		Facebook post privacy		Snapchat location		Apple Family Sharing location	
	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid	Nav	Vid
Addilyn	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y
Cora	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Amara	Y	Y	Y	Y	Y	Y	Y	Y	N/A	N/A
Jen	Y	Y	Y	Y	Y	Y	N/A	N/A	Y	Y

Table 8. Did participants find the information they were looking for? And were the video instructions clear?

Observation 1: Participants were better able to complete instructions with slower videos. Participants no longer mentioned that any of the videos were too fast.

Observation 2: One participant did not realise that the first Snapchat video was a video and not a still image, this was because the play button is a similar colour to the background colour on the Snapchat videos.

Design response: Change background colour for Snapchat videos.

Observation 2 — Snapchat videos' background colour — was modified after the final round of co-evaluation sessions and was not subject to any further evaluation.

The next section looks at participants' qualitative feedback beyond the use of the chatbot to perform a set of information finding scenarios.

6.4.7 QUALITATIVE FEEDBACK

Overall, participants shared positive opinions on the usefulness of the chatbot. In the quote below, a support worker discusses the benefits of using a chatbot to provide technical assistance, as opposed to providing emotional support or legal advice, which she feels would be inappropriate. The support worker also feels positive about the fact that the

chatbot discloses, upfront, its automated nature rather than attempting to seem human.

> *I think it is a great approach to tell people upfront that it is a chatbot. I also appreciate that the type of assistance and topics chosen for the chatbot are well suited to a chatbot. You're not trying to give people emotional support or legal advice, for example, and that feels wise at this point.* [Fleur]

Furthermore, as seen in the quote below, survivors appreciated the effort to address technology-facilitated abuse. Participants were keen to learn more about digital privacy to be able to safeguard themselves and be more certain that they were not unknowingly placing themselves at risk.

> *And it's good that someone is working on that [technical advice] because sometimes people put themselves in danger and they have no idea, they have no clue. It's not that they're doing it intentionally, they don't understand.* [Aria]

Survivors also discussed situations in which they had adjusted their privacy settings but were unsure whether they had achieved the desired outcome. In much the same way as in the interviews and workshops (Chapters 3 and 4), participants were not confident in their own ability to manage privacy settings and were concerned about doing something "wrong". Or in other words, changing their privacy settings and believing their data was protected from the perpetrator when, in fact, the change had not restricted access to their content at all. Having access to the chatbot on Refuge's website gave participants the sense that they could easily follow digital privacy advice from a trusted provider, therefore, removing the risk associated with adjusting privacy settings on their own.

> *Yes, yes, because I'm not so expert in, you know, social media for instance. Sometimes I want to change things and block people, particularly here [in refuge], you know, I don't want people to know I'm here so I block many people and I don't know if I did right. If actually I'm trying to, you know, make the green spot online to not be online for everybody but I never know if I actually did right and if another person is seeing me or not. So yeah, I would use it, for sure.* [Marisole]

Some participants were also of the opinion that the chatbot made it easier and quicker to find information that they would usually have searched for on platforms like YouTube.

> *The navigation is not complex because see, there's not much buttons to press, it's not very complicated at all. It's very simple, I tell you, it's very simple. I find it very helpful. I usually go to the YouTube for any information but this one is just really direct, you*

go here and you can get what you want, just straightforward. Usually you have to go through so many YouTube videos to get what you want but this one is easy. [Farah]

Similarly, a few support workers expressed the opinion that the chatbot was a useful tool to support them in their job, as they felt unable to provide digital privacy advice themselves.

I thought it was really good! Obviously, if you don't have these things — I'm not using that every day, I don't know how to do it — but following the instructions is pretty easy and a bit common sense as well, so, I thought it was really good. Easy. [Hannah]

As expressed in the quote below, in addition to being perceived as useful for support workers and survivors living in refuge, the chatbot was also seen as a helpful tool for survivors seeking support through outreach services. As well as a helpful tool for support workers from other agencies who may not be comfortable in providing digital security advice.

For outreach clients who just require tech support it would be a good tool to signpost to. It would also be helpful for other agencies to use this tool if they are unsure when supporting a client. [Isa]

Particularly because, as one support worker put it, it can be a difficult and time-consuming process to talk through privacy settings over the phone or in-person during support sessions. The chatbot allows survivors to access step-by-step information remotely without the need for a specialised support worker, and in a format that is more appropriate to the information being delivered.

Useful to have a tool that maps out how to change security settings etc., as they can be quite tricky/lengthy to explain. [Mille]

Or even in situations where a victim may not want to speak with a support worker over the phone, as described by Elva below.

When someone wants to access this info quickly without calling anyone. [Elva]

Support workers also appreciated that the chatbot could be used by survivors without supervision in a process of empowering themselves with digital privacy management skills.

In refuges – very useful as we spend a lot of time going through settings on phone etc. with clients – if the clients can access [the] chatbot themselves it would save resources and also give the clients empowerment to make changes themselves. [Juliet]

Furthermore, survivors felt that the chatbot could provide information during crucial times, such as when a survivor goes into refuge. The location of refuges cannot be disclosed and it is, therefore, of paramount importance that survivors' devices are not tracked when going into and staying in refuges.

> *Especially, like, I've been here [in refuge] for about 8 months now so I'm at a place where I'm good but for someone who started out right how I felt at the start, this would've been perfect to help me.* [Cora]

In the sessions and email feedback, participants discussed how the chatbot had made them aware of certain settings and features that they did not know existed. In fact, during some of the co-evaluation scenarios, a few participants asked to use their own phones to ensure that their own settings were "correct". The quotes below illustrate a survivor and a support worker's view on the usefulness of the chatbot for showing survivors privacy features they may have previously been unaware of.

> *Damn, that [Family Sharing] is a good one! I didn't even know that existed. I wish I could do it on my phone [participant's phone had run out of battery].* [Jen]

> *I like the prompts that appear for survivors with support they may need. For some women, they may know they need assistance but they may not know with exactly what, so I found having the prompts really helpful. For example, I clicked iCloud as this is an area I lack knowledge on, then prompts came up to say "Family Sharing", I hadn't realised this was possible so I clicked the link to find out more info.* [Louise]

What is more, participants Cora and Quinn completed some of the scenarios using their own phones as a way of ensuring that their privacy settings were correctly adjusted.

> *Where do you usually find information on your privacy settings?* [Researcher]

> *Just on my phone, just a Google search.* [Cora]

> *Do you think that if it was on the Refuge website that you would use it?* [Researcher]

> *Definitely, rather than the usual way. Now that I know there's the Refuge website! No, very helpful. Especially, like, I've been here for about 8 months now so I'm at a place where I'm good but for someone who started out right how I felt at the start, this would've been perfect to help me.* [Cora]

Participants also felt that the chatbot was easy enough to use that it was not a barrier for less tech-savvy individuals.

That's really easy and simple for people that wouldn't even have a clue and they were starting out just using the internet, like it's just there, it's there, you couldn't ask for more really. [Cora]

Furthermore, participants appreciated the step-by-step nature of the videos, as it removed the complexity of adjusting several privacy settings across different platforms and devices.

No, they are so helpful 'cause they've got all information telling you step-by-step what to do, step-by-step-by-step. [Quinn]

Survivors also offered suggestions on how to improve the chatbot. One of the most common suggestions was to expand on the content offered by the chatbot, such as adding instructional videos for Google Maps.

Because sometimes women don't know they have the locations on, on Google Maps, and they won't know if the alleged perpetrator has access to that email, so they know where she's travelling, or if there's spyware. It's just one of the biggest compromises. [Juliet]

Support workers suggested that the chatbot could be extended to perform other functions other than technical support. In the quote below, Calla describes how the chatbot could provide links to local sources of support based on users' postcode.

Would be great to have something at some point in it, perhaps at the end where you could input your postcode and it would come up with the closest DV service and their contact details. If it's not a Refuge service, then we could give them the DV Helpline and ask them to call to find out. Then it's a more substantial linking in with services. [Calla]

Participants also expressed that audio would be helpful in a series of ways. Some participants suggested that audio instructions would be useful, while others mentioned using audio clues to, for example, indicate when the next step starts. Given that users need to watch the video and then complete the instructions on a mobile device, audio cues would allow the next step to progress without users having to look up from the mobile device or switch between applications.

Not sure if there was any sound with the videos as we have no speakers on the computer we used, but we feel audio description of how to do each step with pauses in between could be greatly helpful. [Niomh]

Maybe the sound so, like when it changes the step. [Marisole]

6.5 CROSS-PLATFORM TESTING

Lastly, Refuge's IT partners and I collaborated on a technical cross-platform evaluation of the chatbot. The cross-platform testing report can be found in Appendix F. The table below outlines issues that were detected in the evaluation and then addressed before the final chatbot went live. Before implementing the changes, all issues and actions points were collaboratively discussed and agreed upon amongst Refuge's Head of Operations, the Technical Lead, and me.

Finding	Issue	Recommendation
Setting icon on Video	Some videos mention the setting icon / app and show it, others just say click settings.	Give a consistent message and explain how to get to the settings icon.
Fullscreen link	Some videos have a full screen message, others do not.	Give a consistent message for full screen. We found no need to show the full screen message.
Menu navigation	Cannot return to the start, you have to click the three lines at the bottom of the screen and click return to main menu.	Needs a restart button on each option, if you choose the wrong phone at the start, you either have to click the three lines or close and start again.
Menu navigation	When in a particular section, such as Facebook, the navigation takes you back to choosing the main topic and then to the section again.	For example, in iPhone, Social Media – Facebook, you have to click the menu 20 times to change each setting. Can the menu be changed so that when you are in a section, you easily click each option, rather than returning to the main menu?
Menu navigation	The main menu asks, "what can I help with" and then the phone type. Once phone type has been chosen, you cannot change it without restarting.	Can we change the menu to ask for phone first and give an option to return to phone type?
Menu navigation	Main menu button does not return to the start	The main menu does not return to main menu, just to a sub menu. Need to redesign the buttons so that sections and start again can be chosen.
YouTube	When a YouTube video has finished, you are presented with adverts for videos which are not relevant.	Consider hosting the videos on the new Helpline web site so that videos do not contain suggestions for other videos at the end.
Videos	The videos do not end with any standard credits.	Should there be a final screen with details of the helpline and how to call it on each video?

Table 9. Results of the cross-device evaluation of the chatbot.

6.6 DISCUSSION

The co-evaluation aimed to collaboratively evaluative the feasibility and acceptability of a fully automated conversational agent, designed to provide digital privacy information and advice to survivors of IPA. In order to do so, the co-evaluation focussed on:

- gathering participants' opinion on the appropriateness of the chatbot to support survivors in managing their digital privacy;
- assessing the effectiveness of the instructional video content and its format for communicating and conveying digital privacy management information;
- iteratively implementing modifications based on participants' feedback;
- iteratively assessing and improving the chatbot's ease-of-use and overall user-experience.

I order to do so, co-evaluation sessions were run with 19 survivors and 9 support workers. Overall, participants had positive opinions of the chatbot, its ease-of-use, and the step-by-step format of the video content. Participants also felt that the chatbot was a useful resource to learn about digital privacy and privacy-related novel features that they may otherwise be unaware of, remotely and whenever they may need it. As described in Section 4.3, during the codesign workshops, one of participants' co-created ideas centred on the development of digital privacy management educational materials. Participants felt that if simple, reliable informational resources were available, this would enable survivors to learn about digital privacy and empower them to safeguard themselves from technology-facilitated IPA. In the co-evaluation participants' opinion, the chatbot has indeed been effective in addressing requirements for educational materials and resources in a simple and easy-to-access format, which allows survivors to take action based on information that they can trust. The information is perceived to be more trustworthy than, for example, tutorials on YouTube since it appears on Refuge's website and Refuge is a trusted DA support organisation.

This work, therefore, demonstrates that codesign with survivors, support workers, and charitable organisations can be effective in creating outcomes that address a shared issue of concern. The issue, in this case, being technology-facilitated IPA and the gap in digital privacy management knowledge experienced by support services and victims. The co-evaluation took place alongside support workers from Refuge and survivors living in Refuge shelters or accessing legal advice at an outreach service. In practice, this means that the co-evaluation reached both survivors living in shelters and those who were not living in shelters. Previous phases of this work had mainly collaborated with survivors not living in refuge, however, it felt important that the chatbot be evaluated with a broader community including survivors living in shelters.

The following sections discuss the process of co-evaluation and my relationship, as a researcher, with Refuge. The discussion is presented through the lens of participatory dynamics and power, pondering the impact these dynamics may have had on the work.

6.6.1 THE EVALUATION OF CODESIGNED OUTCOMES

The formal evaluation of PD projects is a debated subject (Muller, 2007). Authors have previously argued that when participants are included earnestly in the design, development, and implementation of a PD project, an ongoing process of evaluation is already embedded (Bossen, Dindler and Iversen, 2016) and, therefore, formal evaluations are unnecessary. However, from the opposite point-of-view, supporters of the need for formal evaluations of PD argue that built-in forms of evaluation are not robust enough in themselves. Furthermore, they suggest that embedded evaluation methods are not suited to measuring the longer-term impacts of PD interventions (ibid.), beyond the active period of the projects themselves. Muller (2007) argues that, historically, there has been a lack of formal evaluations comparing the outcomes of PD projects with the outcomes of non-PD ones. The emergence of calls for formal PD evaluations has developed as a result of funders and other regulatory organisations' measurement and benchmarking of research (Wilsdon *et al.,* 2015). However, such metrics may not always be suitable for assessing the value contribution of participatory forms of research and design. PD and co-design produce value in diverse forms, over varying periods of time, and across different groups who have diverse agendas (Whitham *et al.,* 2019), making value extremely difficult to capture against a set of largely quantitative metrics.

Maria Escalante (2019) proposes thinking of the PD process in terms of *value constellations* rather than, or in addition to, value chains. In *value constellations*, value emerges across the relationships built within PD between human (and non-human) subjects. Value is thus diffused and displaced across a network or constellation, which does not render itself to being easily measured. Escalante (ibid.) further argues that codesign's value resides in its ability to create space for the emergence of *catalytic encounters* through collaboration. Codesign is therefore not only a site where designs emerge but also relations, affections, and experiences that are never finished or completed but continuously constructed through the processes of relating and collaborating.

Within this PhD, one of the most valuable activities was that of creating relationships and trust between support workers, survivors of abuse, and me. The necessary adaptation of methods and time investment in volunteering, meeting participants, reviewing content

and negotiating expectations, or in other words, *thinking* and relating through the process of codesign is where, I believe, the value of this work lies. It was only through the development of trust and the constant iteration of research materials that the project evolved and assumed its current format, in an ongoing negotiation with participants.

For example, the co-evaluation was *hands-on* and user-experience focussed in its format due to a series of concerns discussed with Refuge, support workers, and survivors during the codesign workshops. Participants concerns related to the nature of research and the perception that their time would not be well spent on theoretical discussions of technology-facilitated abuse or the processes of collaborative design. Participants expressed a vested interest in a form of research that would lead to an outcome, which in turn could be useful to them. Hence, the co-evaluation was focussed on the appropriateness of the chatbot to address participants' real-life current digital privacy management concerns and whether it is usable or not, rather than on discussions of the process itself. An evaluation of the process would rely on the investment of time and resources from participants who are already time- and resource-constrained and who have, in fact, expressed their unwillingness to take part in *"research for the sake of research".* Participants viewed the latter form of research as an activity so far removed from their reality that it had little to no power to affect any change in their circumstances and, therefore, had little willingness to contribute (for free) to it.

What is more, when I approached organisations that had facilitated survivors involvement in previous phases of this work, I found that participants had moved on and it was no longer possible for me to contact them. In this context, as a designer leading the codesign process, it was my obligation to respect participants' expressed desires. What had initially been planned as an exploratory co-evaluation that encompassed both the codesigned outcomes and the codesign process was adapted to a co-evaluation focussed on the practicality of the codesigned tool.

Therefore, the co-evaluation was designed to assess the usability and appropriateness of the chatbot to survivors needs, rather than attempt to quantify the potential value contribution of the chatbot. As argued by Iversen, Halskov, and Leong (2012), as designers and PD practitioners, we must be aware of the ideas of evaluation and value that we propagate when publishing research. It is important that those methods of evaluation are aligned with the values informing the research and are aware of the broader infrastructures (e.g., institutional funding) influencing such evaluations. Fortunately, due to the nature of this PhD funding, we were under no pressure to

perform an evaluation of the PD process that would attempt to quantify the value of the contribution against non-participatory forms of research. Therefore, we had the freedom to make the co-evaluation about assessing the output against participant needs rather than an in-depth evaluation of codesign itself.

6.6.2 CO-EVALUATION, PARTICIPATION, AND POWER

The collaboration with Refuge was an enthusiastic and largely successful one from the point-of-view of the codesign project and designed output. However, from participants' points-of-view, it could be argued that my professional relationship and close collaboration with Refuge management (e.g., the Head of Operations) and staff could lead to the work and myself being associated with institutional power (Palmås and Busch, 2015; Pedersen, 2016). Furthermore, this perceived authority could indeed have been compounded by the perception that the chatbot was owned by Refuge and that, therefore, participants should express favourable opinions of it during the co-evaluation.

Issues of power and perceived authority have been previously discussed in codesign literature and are the subject of ongoing debate within the field, without any clear answer as to how to eradicate power inequalities within codesign projects (Palmås and Busch, 2015; Pedersen, 2016). In fact, PD literature often describes the creation of equal partnerships during collaboration and fails to acknowledge the more complex social dynamics unfolding beneath the surface (Bratteteig and Wagner, 2012; Palmås and Busch, 2015; Pedersen, 2016; Farr, 2018). As observed by Michelle Farr (2018), the attempt to create and report on "equal partnerships" between all those involved in codesign, including staff and service users, can obscure intricate structures and power dynamics that unfold in reality. Such structures are produced by different hierarchies and forms of social inequality that exist beyond the bounds of codesign, which commonly go unacknowledged in the reporting of PD projects.

Within this PhD work, cognisant of the possible perception of my own power as a researcher (Bratteteig and Wagner, 2012; Le Dantec and Fox, 2015) and as a collaborator with Refuge, various efforts to minimise the impact of perceived power were undertaken during the co-evaluation. Firstly, Refuge communicated that participation was entirely voluntary and did not, in any way, affect participants' access to and use of their services. In fact, at all the shelters we visited, less than half the residents expressed interest in participating, which suggests that residents did not feel obliged to take part nor did they feel their access to Refuge services to be threatened. Secondly, during the briefing

sessions, I explained that the chatbot had been a product of collaboration between several groups of survivors and support workers from different organisations and that, therefore, ownership did not belong to me nor would I be offended by any opinions that participants may have expressed regarding chatbot. Thirdly, it was explained that I was not part of Refuge, Refuge had not commissioned the chatbot, nor was anyone being paid for the work being undertaken. Therefore, negative feedback would not have a financial impact on Refuge nor myself as an individual. Finally, the *Tech Champion* introduced her own role as accompanying me to the shelters and outreach services, as an escort necessary to conduct research in these locations, rather than as a collaborator on the project.

However, despite the efforts described above, it is still unclear to which extent participants understood the chatbot as a project being sponsored by Refuge's management or, whether participants were comfortable in giving feedback that could be interpreted as negative. For myself, as a researcher and designer, some questions that remain are, for example:

- *did participants feel comfortable enough to tell us that they did not believe the chatbot met their needs?*
- *did participants feel comfortable enough to suggest an alternative solution that may, in their opinion, be more effective?*
- *did participants feel comfortable enough to question whether resources should've been spent elsewhere?*

These are questions to which I do not have answers. The support of Refuge senior staff may have indeed impacted participants' opinions and evaluation of the chatbot to a greater or lesser extent. However, as with many other codesign projects, we have no reliable way of measuring this effect (Bratteteig *et al.,* 2012). It is nonetheless true that without the full support of Refuge senior management, as a researcher, I would not have had access to the shelters and outreach service. In such a scenario, it is understandable that participants may perceive the researcher and Refuge to more strictly aligned with one another than the researcher and participants. On the other hand, without the demonstration of trust shown by Refuge, in relation to the research, participants would not have been able to take part in this work. Clarke at al. (2019) discuss the myriad ways in which trust is built throughout a codesign process and how it is fundamental to the success of such projects. Within DA, it would not have

been possible to carry out this evaluation alongside survivors living in refuge without Refuge's trust and the my relationship with the organisation.

As a researcher, I too perceived power imbalances between myself and the institution that is Refuge. As a result, at times subconsciously, at other times consciously, I adapted my behaviour in light of what I supposed was expected of my role by Refuge. There was a sense of the fragility of the relationship and an effort to adapt according to Refuge's timelines, availability, and willingness to arrange the co-evaluation sessions. The fragility is perhaps explained by the fact that Refuge, as an organisation, has many concurrent projects, operations, and other factors influencing their availability, which could all change momentarily and have a significant impact on the co-evaluation. As the designer and researcher responsible for the ongoing codesign, I felt it necessary to ensure the collaboration was as effortless for Refuge as possible, therefore, adapting the project timelines and resources to their needs, in order to guarantee continuation.

Other authors have argued that the eradication of power imbalances within codesign is utopian in nature (Le Dantec and Fox, 2015; Farr, 2018; Mulvale *et al.,* 2019). Differences in hierarchy, skills, availability, financial position, and class, to name only a few, cannot be extinguished from the wider context, environment, and actors within which codesign unfolds. Therefore, the results of this co-evaluation should be interpreted in light of the hierarchies of power that may have manifested themselves in myriad ways throughout the process. This does not, however, reduce the significance of the collaborative work undertaken but rather enriches it with a lens of complex social relations within which it is undeniably embedded.

The complexity of involving "vulnerable" participants in codesign has been previously highlighted (Mulvale *et al.,* 2016, 2019; Ssozi-Mugarura, Blake and Rivett, 2017; Spiel *et al.,* 2020). Often, barriers to "vulnerable" groups taking part in research are related to cognitive, communication, conflict management and other skills that some groups may not have had the opportunity to develop, or even time commitments that are seen as too intensive (Mulvale *et al.,* 2019). This was certainly true throughout this PhD. Often participants did not have time to take part or were initially intimidated by the literacy skills they perceived to be necessary. In this co-evaluation, through the development of trust with Refuge, we enabled survivors of DA to take part in shaping a tool that has ultimately been created and launched to address an issue highlighted by themselves as a community. Although power may not have been perfectly balanced between all stakeholder groups, a supportive institutional context was leveraged in such a way

that enabled participants to be involved in shaping a project that may have otherwise been developed without survivors' contribution.

6.6.3 CO-EVALUATION, RESOURCES, AND CHILDCARE

The final points I would like to address in this discussion refer to 1) the (un)availability of childcare and 2) the issue of compensating participants fairly for their time.

Firstly, in retrospect, this project would have benefited from securing funding for childcare during the co-evaluation sessions with survivors. Childcare would have allowed survivors the headspace and time to fully engage in the sessions. Whilst the *Tech Champion* and I supported participants with childcare, participants had a sense that the children were being burdensome to us and, therefore, were concerned about the amount of time that the session was taking. For future work engaging survivors of DA, it seems imperative that budget for childcare is secured and the service is delivered in a format that meets participants' needs.

Secondly, although the Research Ethics Committee decided that participants should not be compensated for their time, I believe that the specific circumstances of DA survivors warrant a more holistic and tailored approach to research participant compensation. Survivors in refuge have fled their homes and have limited access to money and financial support, which are often controlled by the perpetrator. Furthermore, because survivors are living in refuge, finding and maintaining employment is not generally feasible. Survivors find themselves living in a shelter that is not their home, financially dependent on third-sector services, and solely responsible for childcare and maintenance (Bostock, Plumpton and Pratt, 2009). In this context, and based on my experience of working alongside survivors, it is my opinion that the ethical approach would be to compensate participants fairly for their time by offering, for example, an hourly wage or the equivalent in shopping vouchers.

Research participant compensation remains a contentious subject despite a wealth of literature exploring its tenuous impact on research (Permuth-Wey and Borenstein, 2009; Pandya and Desai, 2013; Collins *et al.,* 2017). In the biomedical sciences, research ethics boards have traditionally been concerned that compensation may lead individuals to participate in research out of financial need, which could, in turn, mean that they would be unable to withdraw participation even when confronted with significant health risks. These concerns have prompted institutional restrictions by ethics boards, which have

subsequently led some researchers to provide little or no compensation for research participation (Permuth-Wey and Borenstein, 2009; Collins *et al.,* 2017).

Within PD, the same trends can be observed (Kapuire, Winschiers-Theophilus and Blake, 2015). As discussed by Flicker at al. (2007), often little or no compensation is given to individual participants or community representatives. This further disempowers individuals and communities as it suggests that their time and energy are not as worthy of compensation as the time and energy of the researcher or institutional partners. Furthermore, this approach suggests that individuals and communities should participate solely for the "privilege" of being invited to do so (Flicker *et al.,* 2007), rather than acknowledging their expertise, the cost of their time, and their invaluable contributions to research as partners in codesign.

Within this context, researchers have previously argued that participatory methods can lead to the exploitation of those that are most vulnerable by engaging them in contributing free labour to funded institutional research (Ugalde, 1985; Byrne and Alexander, 2006; Flicker *et al.,* 2007). Although, in some cases, compensation may incentivise participants to take part solely for monetary reasons, it may also enable participation for those who wished to take part but were unable to do so due to time and resource constraints. In cases where researchers are permitted to compensate participants, participatory research projects have taken varied approaches to compensation, from honoraria (Hoeft *et al.,* 2014) to paying for food and other gifts (Hussain, Sanders and Steinert, 2012; Winschiers-Theophilus, Bidwell and Blake, 2012; Hoeft *et al.,* 2014; Duarte *et al.,* 2019). However, compensation does not often accurately reflect the real time cost of participation (Hoeft *et al.,* 2014).

In the case of this work, the REC (Research Ethics Committee) decided that no compensation be given to participants. Therefore, no compensation was given to participants for their time during the interviews or codesign workshops. However, for the co-evaluation, Refuge compensated participants with gift vouchers that could be used for food and other necessities in local high street shops. Refuge assumed a strong position that participants should be compensated for their time, especially since survivors were generous enough to participate in the research whilst going through an unimaginably challenging time in their lives. As a designer and as a researcher, I do not disagree with Refuge's position. In fact, throughout this work, it has been my belief that adequate compensation should be given to participants to fittingly acknowledge their time, effort, and contribution to participatory research and design. Without their

participation, this work would not have been possible. It, therefore, seems unethical to compensate the researcher for her time, allow support workers to participate as part of their daily job-related responsibilities for which they are paid, but not compensate survivors. In fact, research that only involves minimal risk (e.g., does not involve clinical trials, tissue donation, etc.) is not made unethical through the provision of adequate compensation. Rather, it can enhance people's options in terms of participation or non-participation rather than limiting them. Offering survivors appropriate compensation for their time expands their options to travel and take part in research, rather than limiting their ability to give informed consent (Thompson, 1996; Goodman et al., 2004; Andanda, 2009).

What is more, for participatory design PhD research that is not funded, university RECs should ensure that appropriate funds are available to compensate research participants for their time. Whether such compensation is monetary or takes other forms, such as food or shopping vouchers. The aim would be to ensure that community participants are compensated and feel that their time, expertise, and effort is equally as valued as that of research staff and/or other stakeholders taking part in their professional capacities, ensuring that PD processes are not socially exploitative in their structure.

6.7 CONCLUSION

The use of chatbots as a medium capable of delivering information in an always- and remotely-accessible manner has been explored before within sensitive contexts such as DA (Axiom88, 2016; Følstad *et al.,* 2018; Good Hood, 2019). However, such efforts have not been developed alongside survivors of technology-facilitated abuse nor has their effectiveness been evaluated with survivors. This work, therefore, contributes a first attempt at using collaborative design methods to develop a deeper understanding of technology-facilitated IPA, co-create an intervention to address at least an aspect of the broader issue, and co-evaluate the codesigned output alongside survivors and support workers. This chapter specifically addresses the process of co-evaluation with survivors of IPA and support workers, within the context of a collaboration with Refuge, and contributes to existing discussions within PD and HCI with in-context reflections on issues of evaluation (Muller, 2007; Bossen, Dindler and Iversen, 2016; Whitham *et al.,* 2019), power (Thorpe and Gamman, 2011; Le Dantec and Fox, 2015; Palmås and Busch, 2015; Farr, 2018), and participant compensation (Flicker *et al.,* 2007; Steen, 2011; Hoeft *et al.,* 2014; Collins *et al.,* 2017) within PD approaches to research and design.

7

CONCLUSION

This section summarises the contribution and implications of this PhD. It begins with a summary of the overall contributions to knowledge and practice. The next section discusses how the research questions have been addressed, and the chapter closes with an overview of further development and future work.

7.1 CONTRIBUTION TO KNOWLEDGE

This PhD work contributes in the following ways:

- It extends existing knowledge on technology-facilitated IPA, how it is perpetrated, the gaps in existing support provision, and problematizes the need for survivors to be experts in digital privacy management to protect themselves. It does so by building upon existing work conducted in the US and Australia, with perspectives from UK-based NGOs and survivors seeking online peer support.
- This work is, to the best of my knowledge, a first successful attempt to include survivors and support workers in co-creating a tool that tackles the issue of technology-facilitated IPA by providing visual instructional information on digital privacy. A tool that is now owned and updated by an NGO belonging to the community.
- It has also been a first attempt at involving survivors of abuse in anticipating digital privacy threats, which in this case were related to smart homes.

7.2 ADDRESSING THE RESEARCH QUESTIONS

The research questions addressed in this PhD work are listed below.

Can codesign with victims of technology-enabled domestic abuse (DA):

(RQ1) *make a difference to understanding where the system of getting help and support breaks down?*

(RQ2) *help enable the production of viable innovative design solutions to address this national (and global) challenge?*

(RQ3) *inform how design studies understand codesign as a process of generative inquiry in addressing complex social problems?*

The following sections discuss the three research questions in turn, not only in relation to this work but also within the wider context of codesign.

WHERE THE SYSTEM OF GETTING HELP AND SUPPORT BREAKS DOWN (RQ1).

This project is a first attempt to involve survivors and support workers in understanding the complex landscape of technology-facilitated IPA and codesigning support solutions. Through interviews with survivors and support workers, as well as an analysis of online forum data (Chapter 3), this work identified:

- a series of ways through which IPA is currently perpetrated using digital technologies (Chapter 3: Theme 1);
- how survivors are using technology within the context of IPA (Chapter 3: Theme 2);
- the gaps in advice given by NGO support workers regarding digital privacy and security (Chapter 3: Theme 3);
- a gap in survivors' and support workers' knowledge and confidence regarding digital privacy management (Chapter 3: Themes 2 &3).

Following on from the interviews and forum data analysis, which were focussed on understanding the current problem context (Chapter 3), the codesign workshops

then explored a near-future space of smart home technologies (Chapter 4). In collaboration with survivors and support workers, this work developed an understanding of survivors' near-future concerns regarding smart home devices and interpersonal security (Chapter 4: Theme 4), as well as the scenarios in which they envision smart device abuse taking place (Chapter 4: Themes 1 & 2). The workshops also highlighted previously mentioned (Chapter 3) concerns regarding survivors and support workers' self-identified gaps in digital privacy knowledge (Chapter 4: Theme 4) and NGOs' lack of preparedness to deal with such novel threats as those posed by smart homes (Chapter 3: Themes 3 & 4).

Using a codesign approach allowed us to identify where the support provision system breaks down: support workers do not have the knowledge and training necessary to tackle digital privacy and security threats (RQ1). This was true for the current landscape of smartphones and social media but also emerged as a concern that would be made worse by the Internet of Things and smart homes. Survivors and support workers felt that the adoption of smart devices in the home made the work of managing one's digital privacy and security even more complex than it is now, with a plethora of new gadgets, platforms, and privacy settings to effectively manage.

Furthermore, the speculative nature of the workshops, where participants were invited to imagine a near-future home equipped with smart devices, identified a series of interpersonal privacy issues in the design of smart homes. Work in the space of interpersonal privacy and smart homes has begun to emerge (Mennicken and Huang, 2012; Mäkinen, 2016; Rode and Poole, 2018; Geeng and Roesner, 2019; Strengers et al., 2019; Huang, Obada-Obieh and Beznosov, 2020; Tabassum et al., 2020) but it has not yet explored contexts such as domestic abuse where the consequences of technology design flaws may be many degrees more severe. As argued by Mike Monteiro (2019), designers are at least partially responsible for the products they develop and put into the world. The design of smart home devices has been lacking in research on misuse and abuse with diverse audiences that can inform the design and development processes (Rohracher, 2003; Zheng *et al.,* 2018; Strengers *et al.,* 2019). This PhD work contributes to the field by providing the point-of-view of "users" who are commonly excluded from design processes and, therefore underserved or even potentially harmed by novel technologies such as smart home devices.

In summary, a codesign approach with survivors of IPA and support workers has identified several gaps:

- a gap in NGO professionals' training and knowledge on digital privacy, which would enable them to support survivors more confidently;
- a gap in materials and tools to support survivors with digital privacy management;
- a gap in the design of smart home devices, which have historically been targeted at a very specific set of "users" at the cost of exclusion of all others.

Other existing work in Australia and the US has identified similar gaps in support service provision (Dimond, Fiesler and Bruckman, 2011; Woodlock, 2016; Freed *et al.,* 2017; Matthews *et al.,* 2017; Harris and Woodlock, 2018), reporting on similar trends regarding support worker and survivors' confidence and knowledge on digital privacy. However, this is the first study to research and document these findings in a UK NGO context. It is also, to the best of my knowledge, the first to find similar trends in online communities where survivors seek peer-to-peer support and information exchange and may, or may not, be engaged with formalised support services. (Chapter 3). Finally, although existing work has explored issues of interpersonal privacy and smart homes with different types of households, such as shared accommodation (Huang, Obada-Obieh and Beznosov, 2020), my work presents a first attempt at gathering and problematising IPA survivors' concerns regarding these novel technologies.

THE PRODUCTION OF VIABLE INNOVATIVE DESIGN SOLUTIONS TO ADDRESS THIS NATIONAL (AND GLOBAL) CHALLENGE (RQ2).

As previously mentioned, a codesign approach enabled survivors and support workers to collaborate in creating a set of ideas to tackle the issue of technology-facilitated IPA (Chapter 4: Theme 5). Previous work researching technology-facilitated IPA has not involved survivors in problematising and generating ideas to address digital privacy and security issues but has largely focussed on understanding the dynamics and prevalence of the problem (Southworth *et al.,* 2007; Dimond, Fiesler and Bruckman, 2011; Woodlock, 2016; Freed *et al.,* 2017, 2018; Matthews *et al.,* 2017; Chatterjee *et al.,* 2018; Harris and Woodlock, 2018).

The practice-led nature of this PhD has been effective in introducing survivors' voices into designing ideas to address some of the interpersonal privacy concerns enabled by digital technologies. Amongst the codesigned ideas developed by survivors and support workers (Chapter 4: Theme 5), in collaboration with me as a designer/researcher, was that of creating educational materials appropriate to the problem at hand. Participants

identified two main gaps that need to be addressed through educational materials, the first that support workers do not have the necessary knowledge and training to give advice on digital privacy, and the second that survivors do not understand or have the knowledge required to manage a plethora of privacy settings across all their devices.

To address the above-stated problem area, a chatbot was co-developed alongside staff and survivors from Refuge. As described in Chapter 5, the chatbot delivers digital privacy management information in the form of step-by-step videos. The chatbot was evaluated and deployed on Refuge's website where it is now live for survivors to use. Recent usage statistics from 05/09/2020 to 27/11/2020 (90 days) show that 971 people have interacted with the chatbot over this period. Of the top-level menu items, Location Settings was selected 277 times, WhatsApp 269, Social Media 185, iCloud & Apple ID 52 times. From 09/01/2020 to 31/03/2020 (90 days), before the COVID-19 social distancing measures, 164 individual people used the chatbot. This suggests a marked increase in usage which is consistent with media reports on the increase of domestic abuse during the lockdown (Oppenheim, 2020; Townsend, 2020). The remote nature of the chatbot means that survivors of technology-enabled IPA can access it without being engaged with formal support services, as well as without meeting a support worker face-to-face or calling a helpline. The chatbot can be remotely accessed in a more silent, and therefore private manner than, for example, a helpline. In this context, codesign has been effective as a method for understanding the problem area and creating a viable solution to address it (RQ2). Furthermore, a codesign methodology has also been successfully used to create a service that is now owned and given longevity through one of the stakeholder organisations, beyond the involvement of research grant funding. In fact, Refuge is currently translating the chatbot into Polish, Urdu, and Spanish with the intention of reaching more survivors in their native languages.

In addition to the chatbot and to influence the development of smart home devices, this work has also produced a set of guidelines to inform smart home privacy design, which can be accessed here[1]. Furthermore, the results of the interviews, forum data analysis, and workshops have been presented at academic and technology design conferences (Leitão, 2017, 2018b, 2018a, 2019a, 2019b) and used to raise awareness through popular media outlets (Braithwaite, 2018; Harper and Hellen, 2019). As a consequence of those publications, this work has been used to promote awareness of technology-facilitated IPA on technology podcasts, namely Slate's If/Then and the BBC's Digital Human, as well as to promote change within the field of smart home design. Facebook's division for the

1 http://roxanneleitao.com/smarthome/

design and development of smart homes — Portal — has organised for a workshop to be held where I will problematize some of their work with IPA in mind, and collaborate with their designers in tackling identified interpersonal privacy issues. This research has also been presented at Designit in London. Designit is a global design agency specialising in a number of services including the design of digital technologies. In engaging with industry and the people responsible for designing digital services, through this work's findings, I aim to raise awareness of technology-facilitated IPA and offer technologists a way of accessing survivors' experiences and using them to better inform their designs.

In summary, codesign with survivors and support workers has been an effective method of producing a viable design solution to address the issue of technology-facilitated IPA. It has also been effective as a tool for producing a set of findings and guidelines that are being used to raise awareness of the issue amongst technology designers and producers.

CODESIGN AS A PROCESS OF GENERATIVE INQUIRY IN ADDRESSING COMPLEX SOCIAL PROBLEMS (RQ3)

As discussed in the sections above, codesign was effective as a method both for inquiry into the problem space as well as in the co-creation of solutions to address a particular facet — digital privacy management — of the wider issue of technology-facilitated IPA.

In a similar manner to many other codesign projects aimed at tackling complex social problems (Manzini and Coad, 2015), this PhD research involved participants perceived to be "vulnerable" and therefore, required additional thought and preparation to be carried out ethically and sensitively. As Butler *et al.* (2016, p. 1) argue, the concept of vulnerability is socially constructed and *"requires and implies the need for protection",* whilst being tied to notions of victimisation and the inability to take action for oneself. In this context, researchers often see themselves as taking action to "rescue" "vulnerable" individuals or communities through the rhetoric of participatory design and the involvement of "marginalised" groups in projects with institutions who hold more power than participants do, such as universities, the public sector, and NGOs (Butler, Gambetti and Sabsay, 2016).

Björgvinsson and Keshavarz (2020), provide a recent and compelling case-study illustrating how the power dynamics involved in codesign, where the University and public-sector partner defined the scope and aims of a codesign project, ultimately led to the demise of a "marginalised" grassroots community organisation. In their case-

study, the researchers and a partner media company decided to promote a specific leader of the grassroots over the other leaders, due to their institutional agendas and interests, whilst failing to recognise the influence that such behaviour would have on the social relations within the grassroots organisation itself. Although "vulnerability" is often associated with an inability to take action or the need for others to take action on their behalf, that was not the case for the members of this grassroots organisation, nor does it reflect a universal truth (Butler, Gambetti and Sabsay, 2016). The work of Björgvinsson and Keshavarz (ibid.) highlights how codesign projects aimed at addressing social problems, with the best intentions toward a particular "vulnerable" community, may unwittingly provoke negative effects on such communities. In such contexts, an understanding of the community, as well as internal and external power dynamics, is essential to the ethical carrying-out of such projects, as the intervention of researchers – albeit with good intentions — may not be in the best interest of the community (Le Dantec and Fox, 2015; Björgvinsson and Keshavarz, 2020).

I discuss the work of Björgvinsson and Keshavarz (ibid.) because it has relevance to the broader argument that a priori guidelines-based ethics may not always be appropriate, as unforeseen circumstances and dynamics between participants unfold in unexpected ways during participatory research (Flicker *et al.,* 2007; Tutenel, Ramaekers and Heylighen, 2019; Spiel *et al.,* 2020). Ethics boards often grant approval for research based on pre-composed research procedures, consent forms, and information sheets, which is the standard approach to ethics in research and co-design (Guta, Nixon and Wilson, 2013; Munteanu *et al.,* 2015) but does not guarantee the ethical unfolding of a given piece of work. As argued by Preissle and Han (2012, p. 516), *"ethics at best are frameworks that guide decision making. They are not rules, regulations, or laws. Even ethicists who claim absolute values struggle with how those values apply in any given situation".*

Within the context of this PhD, and in the wider context of codesign projects, I believe a *relational* (Ellis, 2007) approach to ethics could have been better suited to the participants and the research. *Relational ethics* recognises the importance of the relationship built between researchers and participants. It aims for a relationship of mutual respect and dignity between researchers, participants, and communities and acknowledges that these relationships change over time. Researchers engaged in *relational ethics* are expected to be true to their characters and values, as well as responsible for their actions and their consequences on others, in constant adaptation as relationships mutate over time (Ellis, 2007). However, with a priori ethics, there is little room for adaptation

once the research has been granted ethical approval. Meaning that procedures devised before the research begins have to be rigidly imposed throughout the research. Within this PhD work, an approach based on the principles of *relational ethics*, in an ongoing dialogue between the researcher (me), participants, and the ethics board, perhaps could have allowed space for:

- acknowledging participants' agency and capacity in negotiating their own terms of participation, rather as passive agents who either agree, or do not agree, to the terms imposed in the Participant Information Sheet and Consent Form;
- negotiating compensation between the University, NGOs, and participants so that the compensation felt fair and just, whilst remaining within limits related to concerns over participant compensation (e.g., participants ignoring risks in favour or monetary compensation) (Pandya and Desai, 2013; Hoeft *et al.,* 2014; Collins *et al.,* 2017);
- reflexively updating the informed consent process for participants who did not understand all the written information in the Participant Information Sheets and Consent forms.

The first bullet point emerges from a belief, based on my experience of conducting this work, that the current approach to ethics deprives participants from becoming truly involved in codesign and taking ownership of their contribution (Flicker *et al.,* 2007; Tutenel, Ramaekers and Heylighen, 2019). A process in which the researcher and the university set the terms of participation and whoever does not agree with them is excluded, creates a dynamic in which the researcher takes information from the participants but does not give them the opportunity for credit nor ownership (Le Dantec and Fox, 2015). Participants' life experiences and stories essentially become the property of the researcher, who is permitted to use that material for academic publication. The researcher is the recipient of credit and career progression, whilst participants often do not gain comparable benefits (Robertson and Wagner, 2013). A *relational* approach to ethics, in which trust is placed on the researcher to negotiate terms of participation with care, rather than relying on *a priori* ethics, allows participants space to voice their opinions on matters of compensation, anonymity, ownership, credit, and levels of involvement, should they wish to do so.

On the second bullet point, as already discussed at more length in Section 5.5, the support workers and I, as a researcher, were compensated for the time we dedicated

to the project, whilst survivors did not receive any compensation. Whilst this feeds into broader arguments of participant compensation in research (Hoeft *et al.,* 2014; Collins *et al.,* 2017), I believe, based on my own experience, that an agreement could have been reached where participants were compensated, at least in some form, for their time whilst not being coerced into participation. Compensation could have been monetary, in the form of food vouchers, or any other form that felt just, but should have demonstrated that we respect and value survivors' time and contribution to the work. A *relational ethics* approach could have allowed for a discussion to take place between the researcher, the NGOs, survivors, and the ethics board with regards to what fair compensation might have looked like within the scope of a PhD research project.

Codesign cannot continue to benefit from the often-free labour of participants to progress academic careers or the interests of public sector collaborators without adequately acknowledging the community individuals that take part both in terms of compensation and acknowledgement (Robertson and Wagner, 2013). As argued by Flicker *et al.* (2007, p. 482), *"[d]espite ethical strictures to avoid creating coercive economic conditions (e.g., offering honoraria so high that economically disadvantaged persons may feel obliged to participate), it is also important to value and compensate all community members on a collaborative team for their time".*

Finally, regarding the third bullet point, during the research and design activities it became clear the information in the Participant Information Sheets and Consent Forms, more often than not, had to be explained verbally either by me or by an NGO staff member. Participants were generally satisfied with the verbal explanation and signed the Consent Form without reading the Participant Information Sheet in much detail. This happened because ethics board requirements for the information in these documents were too complex, and too lengthy, for the literacy levels observed in most participants. In hindsight, these documents could have been simplified to contain only strictly essential information in day-to-day language. For example, detail such as where the data is stored and how to access it was not interesting to participants. All participants wanted to know was that the information was securely stored and that nobody apart from the me and my supervisory team would have access to it.

However, for research materials to be adapted to the particular contexts in which they are used, it would require dynamic ethics review processes that allow researchers the space and freedom to involve participants and ethics boards in open, timely, and ongoing discussions that continually shape the research materials. Although codesign

can be used as a process of generative inquiry into complex and dynamic contexts, it also needs to adapt to the particular ethical challenges that such contexts present, as do the structures and bodies that govern codesign within academia.

7.3 RESEARCH DEVELOPMENT & FUTURE WORK

The interviews phase of this work was limited to only two survivors based in the UK, whilst the other two were based in the US. All NGO staff were based in the UK therefore, the interviews contribute to an understanding of technology-facilitated IPA and support provision in the UK, mainly from the perspective and experience of NGO staff. NGO staff experience gave the study insight not only into support provision but also into survivors' experiences through the retelling of their stories through their support workers. Nonetheless, the interview phase lacked first-person accounts of technology-facilitated IPA in the UK.

The interviews, codesign workshops, and co-evaluation were only performed with survivors engaged with formal support services. This was a requirement from the ethics board but it does mean that we do not have insight into the lives of survivors who had left their abusive partner but had never engaged with professional support provision. On the other hand, the forum data gave the study insight into the experiences of survivors seeking online peer support regarding technology-facilitated IPA, who may not have been engaged with professional support services. However, these survivors were not involved in the collaborative design activities and therefore, did not contribute directly to the final solution.

Furthermore, all the survivors involved in the interviews, codesign workshops, and co-evaluation were female and had been in a heterosexual relationship with the abuser. Although a few of the support workers also supported women in same-sex relationships, the focus of this work was still on heterosexual relationships where the abuser was male. In the future, I aim to extend this work beyond heterosexual relationships to included survivors involved in same-sex relationships.

Finally, given the qualitative design-led nature of this work, my aim is not that the insights be generalisable to a wider population experiencing technology-facilitated IPA. The aim was to understand participants' specific experiences in sufficient detail to design an intervention that may be useful to people going through similar experiences.

In the future, we aim to extend the chatbot to include support on digital privacy management for smart home devices. This has not yet been included due to the fact that smart devices are not widespread in the UK and therefore, by publishing information about these devices we might have been informing abusers as well. Additionally, we aim to translate the chatbot and the instructional videos into a series of languages relevant to the survivor community in the UK, which Refuge has already begun to do and will continue.

In parallel, my aim is to continue advocating within technology design and industry circles, to influence the future design of privacy features and controls for smart home devices.

REFERENCES

Abramson, K. (2014) *'Turning up the Lights on Gaslighting'*, Philosophical Perspectives, 28(1), pp. 1–30. doi: 10.1111/phpe.12046.

Acquisti, A. et al. (2017) *'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online'*, ACM Comput. Surv., 50(3), p. 44:1-44:41. doi: 10.1145/3054926.

AI for Good (2018) rAInbow, rAInbow. Available at: https://www.hirainbow.org/ (Accessed: 28 October 2019).

Amazon (2018) Help: Household Profiles on Alexa Devices, Amazon: Help & Customer Service. Available at: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201628040 (Accessed: 21 September 2018).

Amnesty International (2017) Amnesty reveals alarming impact of online abuse against women, Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ (Accessed: 9 April 2018).

Andanda, P. (2009) *'Vulnerability: Sex Workers in Nairobi's Majengo Slum'*, Cambridge Quarterly of Healthcare Ethics, 18(2), pp. 138–146. doi: 10.1017/S0963180109090239.

Andersen, P. V. K. and Mosleh, W. S. (2020) *'Conflicts in co-design: engaging with tangible artefacts in multi-stakeholder collaboration'*, CoDesign, 0(0), pp. 1–20. doi: 10.1080/15710882.2020.1740279.

Armstrong, L. et al. (2014) Social Design Futures: HEI Research and the AHRC. University of Brighton. Available at: https://mappingsocialdesign.files.wordpress.com/2014/10/social-design-report.pdf.

Atzori, L., Lera, A. and Morabito, G. (2014) *'From "smart objects" to "social objects": The next evolutionary step of the internet of things'*, IEEE Communications Magazine, 52(1), pp. 97–105. doi: 10.1109/MCOM.2014.6710070.

Axiom88 (2016) jael.ai - Artificial Intelligence for Victims of Domestic Violence, Jael. Available at: http://jael.ai/ (Accessed: 28 October 2019).

Babylon (2019) Babylon, Babylon Health. Available at: https://www.babylonhealth.com/ (Accessed: 28 October 2019).

Baird, D. (2015) Sue Perkins takes Twitter break after Top Gear threats, the Guardian. Available at: http://www.theguardian.com/media/2015/apr/14/sue-perkins-twitter-top-gear-jeremy-clarkson (Accessed: 9 April 2018).

Ball, J. (2019) The Double Diamond: A universally accepted depiction of the design process, Design Council. Available at: https://www.designcouncil.org.uk/news-opinion/double-diamond-universally-accepted-depiction-design-process (Accessed: 29 July 2020).

Bardzell, S. (2018) *'Utopias of Participation: Feminism, Design, and the Futures'*, ACM Transactions on Computer-Human Interaction, 25(1), p. 6:1-6:24. doi: 10.1145/3127359.

Bass, E. and Davis, L. (2002) The Courage to Heal: A Guide for Women Survivors of Child Sexual Abuse. Random House.

Batish, R. (2018) Voicebot and Chatbot Design: Flexible conversational interfaces with Amazon Alexa, Google Home, and Facebook Messenger. Packt Publishing Ltd.

Baym, N. K. (2015) Personal connections in the digital age. John Wiley & Sons.

Beeble, M. L., Bybee, D. and Sullivan, C. M. (2010) *'The impact of resource constraints on the psychological well-being of survivors of intimate partner violence over time',* Journal of Community Psychology, 38(8), pp. 943–959.

de la Bellacasa, M. P. (2011) *'Matters of care in technoscience: Assembling neglected things',* Social Studies of Science, 41(1), pp. 85–106. doi: 10.1177/0306312710380301.

Berg, A.-J. (1994) *'A gendered socio-technical construction: the smart house',* in Bringing technology home: gender and technology in a changing Europe. Buckingham: Open University Press.

Bhuyan, R. et al. (2005) *'"Women Must Endure According to Their Karma": Cambodian Immigrant Women Talk About Domestic Violence',* Journal of Interpersonal Violence, 20(8), pp. 902–921

Björgvinsson, E., Ehn, P. and Hillgren, P.-A. (2010) *'Participatory Design and "Democratizing Innovation"',* in Proceedings of the 11th Biennial Participatory Design Conference. New York, NY, USA: ACM (PDC '10), pp. 41–50. doi: 10.1145/1900441.1900448.

Björgvinsson, E., Ehn, P. and Hillgren, P.-A. (2012) *'Agonistic participatory design: working with marginalised social movements',* CoDesign, 8(2–3), pp. 127–144. doi: 10.1080/15710882.2012.672577.

Björgvinsson, E. and Keshavarz, M. (2020) *'Partitioning Vulnerabilities: On the Paradoxes of Participatory Design in the City of Malmö',* in Dancus, A. M., Hyvönen, M., and Karlsson, M. (eds) Vulnerability in Scandinavian Art and Culture. Cham: Springer International Publishing, pp. 247–266. doi: 10.1007/978-3-030-37382-5_12.

Blumenstein, L. and Guadalupe-Diaz, X. (2016) *'Exploration of Intimate Partner Abuse',* in The intersection between intimate partner abuse, technology, and cybercrime: examining the virtual enemy. Durham, North Carolina: Carolina Academic Press, pp. 13–40.

Blythe, M. et al. (2016) *'Anti-Solutionist Strategies: Seriously Silly Design Fiction',* in Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI '16), pp. 4968–4978. doi: 10.1145/2858036.2858482.

Bocij, P. (2004) Cyberstalking: Harassment in the Internet Age and how to Protect Your Family. Greenwood Publishing Group.

Boman, J. and Jevne, R. (2000) *'Ethical Evaluation in Qualitative Research',* Qualitative Health Research, 10(4), pp. 547–554. doi: 10.1177/104973200129118633.

Bossen, C., Dindler, C. and Iversen, O. S. (2016) *'Evaluation in participatory design: a literature survey',* in Proceedings of the 14th Participatory Design Conference: Full papers - Volume 1. Aarhus, Denmark: Association for Computing Machinery (PDC '16), pp. 151–160. doi: 10.1145/2940299.2940303.

Bostock, J., Plumpton, M. and Pratt, R. (2009) *'Domestic violence against women: Understanding social processes and women's experiences',* Journal of Community & Applied Social Psychology, 19(2), pp. 95–110. doi: 10.1002/casp.985.

Bowcott, O. (2020) Family courts not safe for domestic violence victims, lawyers say, the Guardian. Available at: http://www.theguardian.com/law/2020/feb/19/family-courts-not-safe-for-domestic-violence-victims-lawyers-say (Accessed: 23 December 2020).

Bowles, N. (2018) *'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse',* The New York Times, 7 August. Available at: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html (Accessed: 5 January 2019).

Braithwaite, P. (2018) *'Smart home tech is being turned into a tool for domestic abuse',* Wired UK, 22 July. Available at: https://www.wired.co.uk/article/internet-of-things-smart-home-domestic-abuse (Accessed: 1 February 2019).

Bratteteig, T. et al. (2012) *'Organising principles and general guidelines for Participatory Design Projects',* in Routledge Handbook of Participatory Design. Taylor & Francis Group, p. 117.

Bratteteig, T. and Wagner, I. (2012) *'Disentangling power and decision-making in participatory design',* in Proceedings of the 12th Participatory Design Conference: Research Papers - Volume 1. Roskilde, Denmark: Association for Computing Machinery (PDC '12), pp. 41–50. doi: 10.1145/2347635.2347642.

Brem, M. J. et al. (2017) *'Cyber Abuse among Men Arrested for Domestic Violence: Cyber Monitoring Moderates the Relationship between Alcohol Problems and Intimate Partner Violence',* Psychology of Violence. doi: 10.1037/vio0000130.

Brown, D., Ayo, V. and Grinter, R. E. (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. New York, NY, USA: ACM (CHI '14), pp. 1605–1614. doi: 10.1145/2556288.2557119.

Buchan, L. (2017) Women's refuge budgets slashed by nearly a quarter over past seven years, The Independent. Available at: http://www.independent.co.uk/news/uk/politics/women-refuge-budget-cut-quarter-domestic-violence-victims-children-support-a8003066.html (Accessed: 9 April 2018).

Budiu, R. (2018) The User Experience of Chatbots, Nielsen Norman Group. Available at: https://www.nngroup.com/articles/chatbots/ (Accessed: 28 October 2019).

Butler, J., Gambetti, Z. and Sabsay, L. (eds) (2016) *'Introduction',* in Vulnerability in Resistance. Duke University Press, pp. 1–11. doi: 10.1215/9780822373490-001.

Byrne, E. and Alexander, P. M. (2006) *'Questions of Ethics: Participatory Information Systems Research in Community Settings',* in Proceedings of the 2006 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries. Republic of South Africa: South African Institute for Computer Scientists and Information Technologists (SAICSIT '06), pp. 117–126.

Cameron, G. et al. (2017) *'Towards a Chatbot for Digital Counselling',* in Proceedings of the 31st British Computer Society Human Computer Interaction Conference. Swindon, UK: BCS Learning & Development Ltd. (HCI '17), p. 24:1-24:7. doi: 10.14236/ewic/HCI2017.24.

Cameron, G. et al. (2018) *'Best Practices for Designing Chatbots in Mental Healthcare – A Case Study on iHelpr',* in Proceedings of the 32nd International BCS Human Computer Interaction Conference. International BCS Human Computer Interaction Conference, Belfast, UK.

Campbell, J. C. and Lewandowski, L. A. (1997) *'Mental and Physical Health Effects of Intimate Partner Violence on Women and Children',* Psychiatric Clinics, 20(2), pp. 353–374. doi: 10.1016/S0193-953X(05)70317-8.

Charmaz, K. (2014) Constructing Grounded Theory: Introducing Qualitative Methods series. 2nd edn. SAGE Publications.

Chatterjee, R. et al. (2018) *'The Spyware Used in Intimate Partner Violence'*, in 2018 IEEE Symposium on Security and Privacy (SP). 2018 IEEE Symposium on Security and Privacy (SP), pp. 441–458. doi: 10.1109/SP.2018.00061.

Choe, E. K. et al. (2012) *'Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies'*, in Proceedings of the 2012 ACM Conference on Ubiquitous Computing. New York, NY, USA: ACM (UbiComp '12), pp. 61–70. doi: 10.1145/2370216.2370226.

Clarke, R. et al. (2013) *'Digital portraits: photo-sharing after domestic violence'*, in Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, pp. 2517–2526.

Clarke, R. E. et al. (2019) *'Socio-materiality of trust: co-design with a resource limited community organisation'*, CoDesign, 0(0), pp. 1–20. doi: 10.1080/15710882.2019.1631349.

Clement, A. and Besselaar, P. V. den (1993) *'A retrospective look at PD projects'*, Communications of the ACM, 36(4), pp. 29–37.

Coker, A. L. et al. (2000) *'Physical Health Consequences of Physical and Psychological Intimate Partner Violence'*, Archives of Family Medicine, 9(5), p. 451. doi: 10.1001/archfami.9.5.451.

Coleman, F. L. (1997) *'Stalking Behavior and the Cycle of Domestic Violence'*, Journal of Interpersonal Violence, 12(3), pp. 420–432. doi: 10.1177/088626097012003007.

Collins, A. B. et al. (2017) *'"We're giving you something so we get something in return": perspectives on research participation and compensation among people living with HIV who use drugs'*, The International journal on drug policy, 39, pp. 92–98. doi: 10.1016/j.drugpo.2016.09.004.

Conley, H. (2012) *'Economic crisis, austerity and gender equality: The UK case'*, European Gender Equality Law Review, 2, pp. 14–19.

Cook, D. J. (2012) *'How Smart Is Your Home?'*, Science, 335(6076), pp. 1579–1581.

Coyne, R. (2005) *'Wicked problems revisited'*, Design Studies, 26(1), pp. 5–17. doi: 10.1016/j.destud.2004.06.005.

Crisafi, D. N., Mullins, A. R. and Jasinski, J. L. (2016) *'The Rise of the "Virtual Predator": Technology and the Expanding Reach of Intimate Partner Abuse'*, in The intersection between intimate partner abuse, technology, and cybercrime: Examining the virtual enemy. Carolina Academic Press, pp. 97–123.

Cross, N. (1982) *'Designerly ways of knowing'*, Design Studies, 3(4), pp. 221–227. doi: 10.1016/0142-694X(82)90040-0.

Dantec, C. A. L. and DiSalvo, C. (2013) *'Infrastructuring and the formation of publics in participatory design'*, Social Studies of Science, 43(2), pp. 241–264. doi: 10.1177/0306312712471581.

DeKeseredy, W. S. and Schwartz, M. D. (2016) *'Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory'*, Sexualization, Media, & Society, 2(4), p. 2374623816684692. doi: 10.1177/2374623816684692.

Desjardins, A. et al. (2019) *'Alternative Avenues for IoT: Designing with Non-Stereotypical Homes'*, in CHI Conference on Human Factors in Computing Systems Proceedings. CHI 2019, Glasgow, Scotland UK: ACM. doi: https://doi.org/10.1145/3290605.3300581.

Dewey, J. (1927) The public and its problems. Athens: Swallow Press.

Dickson, D. (1977) *'Technology - The Language of Social Action'*, in Design for Need, The Social Contribution of Design. 1st Edition. London: Pergamon Press Ltd., pp. 102–107. Available at: https://www.elsevier.com/books/design-for-need-the-social-contribution-of-design/bicknell/978-0-08-021500-6 (Accessed: 14 February 2018).

Dimond, J. P., Fiesler, C. and Bruckman, A. S. (2011) *'Domestic violence and information communication technologies'*, Interacting with Computers, 23(5), pp. 413–421. doi: 10.1016/j.intcom.2011.04.006.

DiSalvo, C. et al. (2011) *'The collective articulation of issues as design practice'*, CoDesign, 7(3–4), pp. 185–197. doi: 10.1080/15710882.2011.630475.

DiSalvo, C. (2012) Adversarial Design. MIT Press (Design Thinking, Design Theory).

DiSalvo, C., Clement, A. and Pipek, V. (2013) *'Communities: Participatory Design for, with and by communities'*, in Routledge International Handbook of Participatory Design. New York: Routledge, pp. 182–209. doi: 10.4324/9780203108543-15.

Downes, J., Kelly, L. and Westmarland, N. (2014) *'Ethics in Violence and Abuse Research - a Positive Empowerment Approach'*, Sociological Research Online, 19(1), pp. 1–13. doi: 10.5153/sro.3140.

Duarte, A. M. B. et al. (2019) *'Safe spaces in participatory design with young forced migrants'*, CoDesign, 0(0), pp. 1–23. doi: 10.1080/15710882.2019.1654523.

Dudman, J. (2019) *'Want to tackle domestic violence? Then ensure refuges are properly funded | Jane Dudman'*, The Guardian, 21 January. Available at: https://www.theguardian.com/society/2019/jan/21/tackle-domestic-violence-ensure-womens-refuges-funded (Accessed: 8 December 2019).

Ehn, P., Nilsson, E. M. and Topgaard, R. (2014) *'Introduction'*, in Making Futures: Marginal Notes on Innovation, Design, and Democracy. Pelle Ehn, Elisabet M. Nilsson, Richard Topgaard. The MIT Press.

Elks, S. (2018) *'Domestic abusers using internet, smart devices to spy on and control partners, women's group says'*, The Globe and Mail, 29 August. Available at: https://www.theglobeandmail.com/world/article-domestic-abusers-using-internet-smart-devices-to-spy-on-and-control/ (Accessed: 14 September 2018).

Ellis, C. (2007) *'Telling Secrets, Revealing Lives: Relational Ethics in Research With Intimate Others'*, Qualitative Inquiry, 13(1), pp. 3–29. doi: 10.1177/1077800406294947.

Ellsberg, M. et al. (2008) *'Intimate partner violence and women's physical and mental health in the WHO multi-country study on women's health and domestic violence: an observational study'*, The Lancet, 371(9619), pp. 1165–1172. doi: 10.1016/S0140-6736(08)60522-X.

Elsden, C. et al. (2017) *'On Speculative Enactments'*, in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI '17), pp. 5386–5399. doi: 10.1145/3025453.3025503.

Ensmenger, N. (2015) *'"Beards, Sandals, and Other Signs of Rugged Individualism": Masculine Culture within the Computing Professions'*, Osiris, 30(1), pp. 38–65.

Erbaugh, E. B. et al. (2007) *'Queering approaches to intimate partner violence'*, in Gender violence: Interdisciplinary perspectives. NYU Press, pp. 451–459.

Escalante, M. A. L. (2019) *'Framework of emergence: from chain of value to value constellation'*, CoDesign, 15(1), pp. 59–74. doi: 10.1080/15710882.2018.1563616.

Eterovic-Soric, B. et al. (2017) *'Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review'*, Computers & Security, 70, pp. 278–289. doi: 10.1016/j.cose.2017.06.008.

European Commission (2016) Advancing the Internet of Things in Europe. EUR-Lex-52016SC0110-EN-EUR-Lex. Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110 (Accessed: 18 June 2019).

Evans, W. and Rangarajan, S. (2017) Hidden figures: How Silicon Valley keeps diversity data secret, Reveal. Available at: https://www.revealnews.org/article/hidden-figures-how-silicon-valley-keeps-diversity-data-secret/ (Accessed: 20 March 2018).

Faily, S., Parkin, S. J. and Lyle, J. (2012) *'Secure System? Challenge Accepted: Finding and Resolving Security Failures Using Security Premortems'*, in. The 26th BCS Conference on Human Computer Interaction (HCI), Birmingham, UK: BCS Learning & Development. doi: 10.14236/ewic/HCI2012.66.

Farr, M. (2018) *'Power dynamics and collaborative mechanisms in co-production and co-design processes'*, Critical Social Policy, 38(4), pp. 623–644. doi: 10.1177/0261018317747444.

Fitzpatrick, K. K., Darcy, A. and Vierhile, M. (2017) *'Delivering Cognitive Behavior Therapy to Young Adults With Symptoms of Depression and Anxiety Using a Fully Automated Conversational Agent (Woebot): A Randomized Controlled Trial'*, JMIR Mental Health, 4(2), p. e19. doi: 10.2196/mental.7785.

Flicker, S. et al. (2007) *'Ethical Dilemmas in Community-Based Participatory Research: Recommendations for Institutional Review Boards'*, Journal of Urban Health : Bulletin of the New York Academy of Medicine, 84(4), pp. 478–493. doi: 10.1007/s11524-007-9165-7.

Følstad, A. et al. (2018) *'SIG: Chatbots for Social Good'*, in Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI EA '18), p. SIG06:1-SIG06:4. doi: 10.1145/3170427.3185372.

Følstad, A. and Brandtzæg, P. B. (2017) *'Chatbots and the New World of HCI'*, Interactions, 24(4), pp. 38–42. doi: 10.1145/3085558.

Foucault, M. (1977) Discipline and punish: the birth of the prison. London: Allen Lane.

Franceschi-Bicchierai, L. and Cox, J. (2017) Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones, Motherboard. Available at: https://motherboard.vice.com/en_us/article/inside-stalkerware-surveillance-market-flexispy-retina-x (Accessed: 23 April 2017).

Freed, D. et al. (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), p. 46:1-46:22. doi: 10.1145/3134681.

Freed, D., Palmer, J., Minchala, D., et al. (2018) *'"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology'*, in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI '18), p. 667:1-667:13. doi: 10.1145/3173574.3174241.

Freed, D., Palmer, J., Ristenpart, D., et al. (2018) '"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology'.

Gamman, L. and Thorpe, A. (2011) *'Criminality and Creativity: What's at Stake in Designing Against Crime?'*, in Clarke, A. J. (ed.) Design Anthropology: Object Culture in the 21st Century. Vienna: Springer (Edition Angewandte), pp. 56–71. doi: 10.1007/978-3-7091-0234-3_5.

Geeng, C. and Roesner, F. (2019) *'Who's In Control?: Interactions In Multi-User Smart Homes'*, in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI 2019, Glasgow, Scotland UK. doi: https://doi.org/10.1145/3290605.3300498.

Giménez-Nadal, J. I., Mangiavacchi, L. and Piccoli, L. (2019) *'Keeping inequality at home: The genesis of gender roles in housework'*, Labour Economics, 58, pp. 52–68. doi: 10.1016/j.labeco.2019.03.006.

Giordano, J. et al. (2007) *'Confidentiality and Autonomy: The Challenge(s) of Offering Research Participants a Choice of Disclosing Their Identity'*, Qualitative Health Research, 17(2), pp. 264–275. doi: 10.1177/1049732306297884.

Good Hood (2019) Hello Cass, Hello Cass. Available at: http://hellocass.com.au (Accessed: 28 October 2019).

Goodman, L. A. et al. (2004) *'Training counseling psychologists as social justice agents: Feminist and multicultural principles in action'*, The counseling psychologist, 32(6), pp. 793–836.

Google (2018) Set up multiple users for your speaker, Google Home Help. Available at: https://support.google.com/googlehome/answer/7323910?hl=en (Accessed: 21 September 2018).

Google (2019) Dialogflow, Dialogflow. Available at: https://dialogflow.com/ (Accessed: 28 October 2019).

Goulden, M. et al. (2018) *'Living with interpersonal data: Observability and accountability in the age of pervasive ICT'*, New Media & Society, 20(4), pp. 1580–1599. doi: 10.1177/1461444817700154.

Goulden, M. (2019) *'"Delete the family": platform families and the colonisation of the smart home'*, Information, Communication & Society, 0(0), pp. 1–18. doi: 10.1080/1369118X.2019.1668454.

Government Equalities Office (2015) Hundreds of victims of revenge porn seek support from helpline, GOV.UK. Available at: https://www.gov.uk/government/news/hundreds-of-victims-of-revenge-porn-seek-support-from-helpline (Accessed: 9 March 2018).

Grierson, J. (2018) Police taking days to respond to 999 calls as budget cuts bite, The Guardian. Available at: http://www.theguardian.com/uk-news/2018/mar/22/police-taking-days-to-respond-to-999-calls-as-budget-cuts-bite (Accessed: 22 March 2018).

Grigg, D. W. (2010) *'Cyber-Aggression: Definition and Concept of Cyberbullying'*, Journal of Psychologists and Counsellors in Schools, 20(2), pp. 143–156. doi: 10.1375/ajgc.20.2.143.

Grinyer, A. (2009) *'The anonymity of research participants: Assumptions, ethics, and practicalities'*, Pan, 12(1), pp. 49–58.

Guta, A., Nixon, S. A. and Wilson, M. G. (2013) *'Resisting the seduction of "ethics creep": Using Foucault to surface complexity and contradiction in research ethics review'*, Social Science & Medicine, 98, pp. 301–310. doi: 10.1016/j.socscimed.2012.09.019.

Hall, A. (2016) Behind Closed Doors. True Vision. Available at: http://truevisiontv.com/films/details/286/behind-closed-doors (Accessed: 12 November 2017).

Halskov, K. and Dalsgaard, P. (2007) *'The emergence of ideas: the interplay between sources of inspiration and emerging design concepts'*, CoDesign, 3(4), pp. 185–211.

Hargreaves, T., Wilson, C. and Hauxwell-Baldwin, R. (2018) *'Learning to live in a smart home'*, Building Research & Information, 46(1), pp. 127–139. doi: 10.1080/09613218.2017.1286882.

Harper, T. and Hellen, N. (2019) *'Smart gadgets open door to stalking and abuse, say police'*, The Sunday Times, 13 January. Available at: https://www.thetimes.co.uk/article/smart-gadgets-open-door-to-stalking-and-abuse-say-police-5xk8n7r9m (Accessed: 1 February 2019).

Harris, B. A. and Woodlock, D. (2018) *'Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies'*, The British Journal of Criminology. doi: 10.1093/bjc/azy052.

Harrison, S. (2019) *'Five Years of Tech Diversity Reports—and Little Progress'*, Wired, 10 January. Available at: https://www.wired.com/story/five-years-tech-diversity-reports-little-progress/ (Accessed: 29 July 2020).

Hazas, M. and Strengers, Y. (2019) *'Promoting Smart Homes'*, in Energy Fables: Challenging Ideas in the Energy Sector. Routledge, p. 78.

He, W. et al. (2018) *'Rethinking access control and authentication for the home internet of things (iot)'*, in 27th USENIX Security Symposium USENIX Security 18, pp. 255–272. Available at: https://www.usenix.org/conference/usenixsecurity18/presentation/he.

HealthTalk (2017) Overview | Women's experiences of Domestic Violence and Abuse, Domestic Violence & Abuse, People's Experiences | healthtalk.org. Available at: http://www.healthtalk.org/peoples-experiences/domestic-violence-abuse/womens-experiences-domestic-violence-and-abuse/overview (Accessed: 1 November 2017).

Her Majesty's Inspectorate of Constabulary and HM Crown Prosecution Service Inspectorate (2017) Living in fear – the police and CPS response to harassment and stalking. 978-1-78655-414–7. Her Majesty's Inspectorate of Constabulary & Her Majesty's Prosecution Service Inspectorate. Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf.

Herman, J. L. (2015) Trauma and recovery: The aftermath of violence — from domestic abuse to political terror. New York, NY, US: Basic Books.

HM Government (2014) A Call to End Violence against Women and Girls: Action Plan 2014.

HM Government (2016) Ending violence against Women and Girls: Strategy 2016-2020. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/522166/VAWG_Strategy_FINAL_PUBLICATION_MASTER_vRB.PDF (Accessed: 17 November 2016).

Hoeft, T. J. et al. (2014) *'Building partnerships in community-based participatory research: Budgetary and other cost considerations'*, Health promotion practice, 15(2), pp. 263–270. doi: 10.1177/1524839913485962.

Holt, T. J. and Bossler, A. M. (2015) Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. Routledge.

Home Office (2015) 'Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/482528/Controlling_or_coercive_behaviour_-_statutory_guidance.pdf.

Hoonaard, W. C. van den (2003) *'Is Anonymity an Artifact in Ethnographic Research?'*, Journal of Academic Ethics, 1(2), pp. 141–151. doi: 10.1023/B:JAET.0000006919.58804.4c.

Huang, Y., Obada-Obieh, B. and Beznosov, K. (2020) *'Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks'*, in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu, HI, USA: Association for Computing Machinery (CHI '20), pp. 1–13. doi: 10.1145/3313831.3376529.

Hunter, R., Burton, M. and Trinder, L. (2020) Assessing Risk of Harm to Children and Parents in Private Law Children Cases. Ministry of Justice. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/895173/assessing-risk-harm-children-parents-pl-childrens-cases-report_.pdf.

Hussain, S., Sanders, E. B.-N. and Steinert, M. (2012) *'Participatory Design with Marginalized People in Developing Countries: Challenges and Opportunities Experienced in a Field Study in Cambodia'*, International Journal of Design, 6(2). Available at: http://128.199.168.50/index.php/IJDesign/article/view/1054 (Accessed: 9 February 2020).

IBM (2018) Watson Assistant | IBM Cloud, Watson Assistant. Available at: https://www.ibm.com/cloud/watson-assistant/ (Accessed: 28 October 2019).

IDAS (2019) Safety Plan, IDAS: Safety Plan. Available at: https://www.idas.org.uk/our-services/domestic-abuse/safety-plan/ (Accessed: 23 April 2019).

Iversen, O. S., Halskov, K. and Leong, T. W. (2012) *'Values-led participatory design'*, CoDesign, 8(2–3), pp. 87–103. doi: 10.1080/15710882.2012.672575.

Jakobi, T. et al. (2017) *'The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study'*, in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI '17), pp. 1620–1633. doi: 10.1145/3025453.3025799.

Janarthanam, S. (2017) Hands-On Chatbots and Conversational UI Development: Build chatbots and voice user interfaces with Chatfuel, Dialogflow, Microsoft Bot Framework, Twilio, and Alexa Skills. Packt Publishing Ltd.

Jang, W., Chhabra, A. and Prasad, A. (2017) *'Enabling Multi-user Controls in Smart Home Devices'*, in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. New York, NY, USA: ACM (IoTS&P '17), pp. 49–54. doi: 10.1145/3139937.3139941.

Johnson, M. P. (2010) A Typology of Domestic Violence: Intimate Terrorism, Violent Resistance, and Situational Couple Violence. UPNE.

Jones, O. (2014) Britain is going backwards on violence against women, The Guardian. Available at: https://www.theguardian.com/commentisfree/2014/mar/30/britain-violence-against-women-domestic-abuse-funding-cuts (Accessed: 12 November 2015).

Kapuire, G. K., Winschiers-Theophilus, H. and Blake, E. (2015) *'An insider perspective on community gains: A subjective account of a Namibian rural communities perception of a long-term participatory design project'*, International Journal of Human-Computer Studies, 74, pp. 124–143. doi: 10.1016/j.ijhcs.2014.10.004.

Kelly, J. B. and Johnson, M. P. (2008) *'Differentiation among types of intimate partner violence: Research update and implications for interventions'*, Family court review, 46(3), pp. 476–499.

Kensing, F. and Blomberg, J. (1998) *'Participatory Design: Issues and Concerns'*, Computer Supported Cooperative Work (CSCW), 7(3), pp. 167–185. doi: 10.1023/A:1008689307411.

Kesharwani, A. (2020) *'Do (how) digital natives adopt a new technology differently than digital immigrants? A longitudinal study'*, Information & Management, 57(2), p. 103170. doi: 10.1016/j.im.2019.103170.

Kimmel, M. S. (2002) *'"Gender Symmetry" in Domestic Violence: A Substantive and Methodological Research Review'*, Violence Against Women, 8(11), pp. 1332–1363. doi: 10.1177/107780102237407.

Kolko, J. (2009) *'Abductive Thinking and Sensemaking: The Drivers of Design Synthesis'*, Design Issues, 26(1), pp. 15–28. doi: 10.1162/desi.2010.26.1.15.

Kretzschmar, K. et al. (2019) *'Can Your Phone Be Your Therapist? Young People's Ethical Perspectives on the Use of Fully Automated Conversational Agents (Chatbots) in Mental Health Support'*, Biomedical Informatics Insights, 11, p. 1178222619829083. doi: 10.1177/1178222619829083.

Latour, B. (2004) *'Why Has Critique Run out of Steam? From Matters of Fact to Matters of Concern'*, Critical Inquiry, 30(2), pp. 225–248. doi: 10.1086/421123.

Latour, B. (2008) *'What is the style of matters of concern?'*, Two lectures in empirical philosophy. Department of Philosophy of the University of Amsterdam, Amsterdam: Van Gorcum. Available at: http://www.bruno-latour.fr/sites/default/files/97-SPINOZA-GB.pdf.

Laville, S. (2016) *'Revenge porn decision sparks anger at police'*, The Guardian, 8 May. Available at: https://www.theguardian.com/technology/2016/may/08/revenge-porn-decision-sparks-anger-at-police (Accessed: 10 October 2017).

Laxton, C. (2014) *'Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking'*, in. Women's Aid. Available at: https://www.womensaid.org.uk/virtual-world-real-fear/ (Accessed: 13 December 2016).

Le Dantec, C. (2012) *'Participation and Publics: Supporting Community Engagement'*, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI '12), pp. 1351–1360. doi: 10.1145/2207676.2208593.

Le Dantec, C. A. and Fox, S. (2015) *'Strangers at the Gate: Gaining Access, Building Rapport, and Co-Constructing Community-Based Research'*, in Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. New York, NY, USA: ACM (CSCW '15), pp. 1348–1358. doi: 10.1145/2675133.2675147.

Lehtonen, T.-K. (2003) *'The Domestication of New Technologies as a Set of Trials'*, Journal of Consumer Culture, 3(3), pp. 363–385. doi: 10.1177/14695405030033014.

Leitão, R. (2017) *'Personal Data Gathering in the Built Environment: a Domestic Abuse Perspective'*, in People, Personal Data and the Built Environment workshop. DIS '17: Conference on Designing Interactive Systems, Edinburgh, United Kingdom: Association for Computing Machinery. doi: https://dl.acm.org/doi/10.1145/3064857.3064864.

Leitão, R. (2018a) 'Design Fictions and Extreme Users'. Mozfest/2018, London, United Kingdom, 22 October. Available at: https://www.mozillafestival.org/en/.

Leitão, R. (2018b) *'Digital Technologies and their Role in Intimate Partner Violence'*, in Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI EA '18), pp. 1–6. doi: 10.1145/3170427.3180305.

Leitão, R. (2019a) *'Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse'*, in Proceedings of the 2019 on Designing Interactive Systems Conference.

New York, NY, USA: Association for Computing Machinery (DIS '19), pp. 527–539. doi: 10.1145/3322276.3322366.

Leitão, R. (2019b) 'Intimate partner abuse facilitated by wearables and smart home devices: survivors and support workers' concerns, requirements, and understanding of smart device privacy and security'. 3rd European Conference on Domestic Violence, Oslo, Norway, 1 September. Available at: https://ecdv-oslo.org/files/2019/08/ECDV-Conference2019-WEB.pdf.

Levine, C. et al. (2004) *'The Limitations of "Vulnerability" as a Protection for Human Research Participants'*, The American Journal of Bioethics, 4(3), pp. 44–49. doi: 10.1080/15265160490497083.

Lyndon, A., Bonds-Raacke, J. and Cratty, A. D. (2011) *'College Students' Facebook Stalking of Ex-Partners'*, Cyberpsychology, Behavior, and Social Networking, 14(12), pp. 711–716. doi: 10.1089/cyber.2010.0588.

Mäkinen, L. A. (2016) *'Surveillance On/Off: Examining Home Surveillance Systems From The User's Perspective'*, Surveillance and Society, 14(1), pp. 59–77.

Mantilla, K. (2013) *'Gendertrolling: Misogyny Adapts to New Media'*, Feminist Studies, 39(2), pp. 563–570.

Manzini, E. and Coad, R. (2015) Design, When Everybody Designs: An Introduction to Design for Social Innovation. MIT Press. Available at: https://books.google.co.uk/books?id=VVrcoAEACAAJ.

Marganski, A. and Melander, L. (2015) *'Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association With In-Person Dating Violence'*, Journal of Interpersonal Violence, p. 0886260515614283. doi: 10.1177/0886260515614283.

Matczak, A., Hatzidimitriadou, E. and Lindsay, J. (2011) Review of domestic violence policies in England & Wales. Kingston University and St George's, University of London.

Mattelmäki, T. and Visser, F. S. (2011) *'Lost in Co-X: Interpretations of Co-design and Co-creation'*, in. 4th Conference on Design Research, Delft, Netherlands, pp. 1–12. Available at: https://mycourses.aalto.fi/pluginfile.php/486475/course/section/101167/mattelmaki_lost-in-cox_fin-1.pdf.

Matthews, T. et al. (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. New York, NY, USA: ACM (CHI '17), pp. 2189–2201. doi: 10.1145/3025453.3025875.

McIntyre-Mills, J. (2010) *'Participatory Design for Democracy and Wellbeing: Narrowing the Gap Between Service Outcomes and Perceived Needs'*, Systemic Practice and Action Research, 23(1), pp. 21–45. doi: 10.1007/s11213-009-9145-9.

Megarry, J. (2014) *'Online incivility or sexual harassment? Conceptualising women's experiences in the digital age'*, Women's Studies International Forum, 47, pp. 46–55. doi: 10.1016/j.wsif.2014.07.012.

Melander, L. A. (2010) *'College Students' Perceptions of Intimate Partner Cyber Harassment'*, CyberPsychology, Behavior & Social Networking, 13(3), pp. 263–268.

Mennicken, S. and Huang, E. M. (2012) *'Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them'*, in Kay, J. et al. (eds)

Pervasive Computing. Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 143–160.

Merrill, N. (2020) *'Security Fictions: Bridging Speculative Design and Computer Security'*, in Proceedings of the 2020 ACM Designing Interactive Systems Conference. New York, NY, USA: Association for Computing Machinery (DIS '20), pp. 1727–1735. doi: 10.1145/3357236.3395451.

Michel, R. (2007) Design Research Now: Essays and Selected Projects. Walter de Gruyter.

Mindshare (2016) 'Human in the Machine'. Mindshare. Available at: https://www.mindshareworld.com/sites/default/files/MINDSHARE_HUDDLE_HUMANITY_MACHINE_2016_0.pdf (Accessed: 20 October 2019).

Miner, A. S. et al. (2016) *'Smartphone-Based Conversational Agents and Responses to Questions About Mental Health, Interpersonal Violence, and Physical Health'*, JAMA Internal Medicine, 176(5), pp. 619–625. doi: 10.1001/jamainternmed.2016.0400.

Monteiro, M. (2019) Ruined by Design: How Designers Destroyed the World, and What We Can Do to Fix It. Independently Published.

Moore, R. J. and Arar, R. (2018) *'Conversational UX Design: An Introduction'*, in Moore, R. J. et al. (eds) Studies in Conversational UX Design. Cham: Springer International Publishing (Human–Computer Interaction Series), pp. 1–16. doi: 10.1007/978-3-319-95579-7_1.

van Moorsel, A. et al. (2011) Digital Strategy for the Social Inclusion of Survivors of Domestic Violence. Research Report CS-TR-1277. Available at: https://kar.kent.ac.uk/58714/1/TR1277.pdf.

Mouffe, C. (2005) The return of the political. Verso. Available at: https://books.google.co.uk/books?hl=en&lr=&id=ApKFSeQE-HMC&oi=fnd&pg=PP8&dq=chantal+mouffe&ots=m5NvZ2OChy&sig=irTGBKygt5Wab3DfnzoVZMFON9g (Accessed: 10 February 2017).

Mulla, S. and Hlavka, H. (2011) *'Gendered Violence and the Ethics of Social Science Research'*, Violence Against Women, 17(12), pp. 1509–1520. doi: 10.1177/1077801211436169.

Muller, M. J. (2007) *'Participatory design: the third space in HCI'*, in The human-computer interaction handbook. CRC press, pp. 1087–1108.

Mulvale, A. et al. (2016) *'Applying experience-based co-design with vulnerable populations: Lessons from a systematic review of methods to involve patients, families and service providers in child and youth mental health service improvement'*, Patient Experience Journal, 3(1), pp. 117–129. doi: 10.35680/2372-0247.1104.

Mulvale, G. et al. (2019) *'Codesigning health and other public services with vulnerable and disadvantaged populations: Insights from an international collaboration'*, Health Expectations, 22(3), pp. 284–297. doi: 10.1111/hex.12864.

Munro, K. (2018) *'Unwaged Work and the Production of Sustainability in Eco-Conscious Households'*, Review of Radical Political Economics, 50(4), pp. 675–682. doi: 10.1177/0486613418767457.

Munteanu, C. et al. (2015) *'Situational Ethics: Re-thinking Approaches to Formal Ethics Requirements for Human-Computer Interaction'*, in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI '15), pp. 105–114. doi: 10.1145/2702123.2702481.

Newman, E. and Kaloupek, D. (2009) *'Overview of research addressing ethical dimensions of participation in traumatic stress studies: Autonomy and beneficence'*, Journal of Traumatic Stress, 22(6), pp. 595–602. doi: 10.1002/jts.20465.

Nicolaidis, C. (2002) *'The Voices of Survivors Documentary: Using Patient Narrative to Educate Physicians About Domestic Violence'*, Journal of General Internal Medicine, 17(2), pp. 117–124. doi: 10.1046/j.1525-1497.2002.10713.x.

NNEDV (2019) Technology Safety, Technology Safety. Available at: https://www.techsafety.org (Accessed: 28 October 2019).

Noble, S. and Roberts, S. (2019) *'Technological Elites, the Meritocracy, and Postracial Myths in Silicon Valley'*, in Mukherjee, R., Banet-Weiser, S., and Gray, H. (eds) Racism Postrace. Duke University Press, pp. 113–129. doi: 10.1215/9781478003250-008.

Nuttall, J. (1972) *'How to Use Technology'*, in Design Participation. Design Research Society's Conference, Manchester, UK: Academy Editions.

Nyborg, S. and Røpke, I. (2011) *'Energy impacts of the smart home-conflicting visions'*, in Energy impacts of the smart home-conflicting visions. European Council for an Energy Efficient Economy.

Odyssey Networks (2013) Domestic Violence: Nicole's Story. Available at: https://www.youtube.com/watch?v=0Dmc7EpaR4g (Accessed: 12 November 2017).

Office for National Statistics (2016) Intimate personal violence and partner abuse, Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/compendium/focusonviolentcrimeandsexualoffences/yearendingmarch2015/chapter4intimatepersonalviolenceandpartnerabuse (Accessed: 15 February 2017).

Office for National Statistics (2017a) Compendium: Domestic abuse, sexual assault and stalking. Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/compendium/focusonviolentcrimeandsexualoffences/yearendingmarch2016/domesticabusesexualassaultandstalking (Accessed: 7 March 2018).

Office for National Statistics (2017b) Domestic abuse in England and Wales: year ending March 2017, Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2017 (Accessed: 13 January 2018).

Oppenheim, M. (2018) Austerity cuts leave domestic violence victims facing toughest Christmas yet, The Independent. Available at: https://www.independent.co.uk/news/uk/home-news/domestic-violence-victims-christmas-therapeutic-support-victims-cuts-refuges-womens-aid-a8673071.html (Accessed: 8 December 2019).

Oppenheim, M. (2019) Police accused of 'systemic failure' to protect victims of domestic abuse and sexual violence, The Independent. Available at: https://www.independent.co.uk/news/uk/crime/police-super-complaint-domestic-violence-sexual-violence-centre-women-s-justice-a8830366.html (Accessed: 23 December 2020).

Oppenheim, M. (2020) *'Visits to national domestic abuse helpline website surge by 950 per cent during lockdown'*, The Independent, 27 May. Available at: https://www.independent.co.uk/news/uk/home-news/coronavirus-uk-domestic-abuse-helpline-calls-rise-refuge-a9534591.html (Accessed: 4 July 2020).

Packham, A. (2020) Revenge Porn Helpline Cases Surge In Lockdown, With 'Sextortion' On Rise, HuffPost UK. Available at: https://www.huffingtonpost.co.uk/entry/revenge-porn-helpline-cases-surge-in-lockdown_uk_5f620ff7c5b68d1b09ca70fb (Accessed: 28 December 2020).

PACT Care BV (2019) Florence, Florence - Your health assistant. Available at: https://www.florence.chat/ (Accessed: 28 October 2019).

Palmås, K. and Busch, O. von (2015) *'Quasi-Quisling: co-design and the assembly of collaborateurs'*, CoDesign, 11(3–4), pp. 236–249. doi: 10.1080/15710882.2015.1081247.

Pandya, M. and Desai, C. (2013) *'Compensation in clinical research: The debate continues'*, Perspectives in Clinical Research, 4(1), pp. 70–74. doi: 10.4103/2229-3485.106394.

Papacharissi, Z. (2015) Affective Publics: Sentiment, Technology, and Politics. Oxford University Press.

Papanek, V. J. (1972) Design for the real world. London: Thames and Hudson.

Pedersen, J. (2016) *'War and peace in codesign'*, CoDesign, 12(3), pp. 171–184.

Pence, E. and Paymar, M. (1993) Education Groups for Men Who Batter: The Duluth Model. Springer Publishing Company.

Perez, C. C. (2019) Invisible Women: Exposing Data Bias in a World Designed for Men. 1st edn. Penguin.

Permuth-Wey, J. and Borenstein, A. R. (2009) *'Financial Remuneration for Clinical and Behavioral Research Participation: Ethical and Practical Considerations'*, Annals of Epidemiology, 19(4), pp. 280–285. doi: 10.1016/j.annepidem.2009.01.004.

Pew Research Center (2012) *'Global Digital Communication: Texting, Social Networking Popular Worldwide'*, Pew Research Center's Global Attitudes Project, 29 February. Available at: http://www.pewglobal.org/2011/12/20/global-digital-communication-texting-social-networking-popular-worldwide/ (Accessed: 7 March 2018).

Preissle, J. and Han, Y. (2012) *'Feminist Research Ethics'*, in Hesse-Biber, S., Handbook of Feminist Research: Theory and Praxis. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., pp. 583–605. doi: 10.4135/9781483384740.n28.

Rangarajan, S. and Evans, W. (2017) *'How we analyzed Silicon Valley tech companies' diversity data'*, Reveal. Available at: https://www.revealnews.org/article/how-we-analyzed-silicon-valley-tech-companies-diversity-data/ (Accessed: 20 March 2018).

Refuge (2017) Our history, Refuge Charity - Domestic Violence Help. Available at: https://www.refuge.org.uk/our-story/our-history/ (Accessed: 28 October 2019).

Refuge (2020) *'72% of Refuge service users identify experiencing tech abuse'*, Refuge Charity - Domestic Violence Help, 9 January. Available at: https://www.refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/ (Accessed: 29 July 2020).

Rice, L. (2017) *'Nonhumans in participatory design'*, CoDesign, 0(0), pp. 1–20. doi: 10.1080/15710882.2017.1316409.

Richards, L. (2016) Domestic Abuse, Stalking and Harassment and Honour Based Violence (DASH, 2009-16) Risk Identification and Assessment and Management Model. National Police Chiefs' Council & Safe Lives. Available at: https://www.dashriskchecklist.co.uk/wp-content/uploads/2016/09/DASH-2009-2016-with-quick-reference-guidance.pdf.

Rittel, H. W. and Webber, M. M. (1973) *'Dilemmas in a general theory of planning'*, Policy sciences, 4(2), pp. 155–169.

Robertson, T. and Simonsen, J. (2012) *'Participatory Design: An Introduction'*, in Routledge International Handbook of Participatory Design. London: Routledge, pp. 1–18.

Robertson, T. and Wagner, I. (2013a) *'Ethics: engagement, representation and politics-in-action'*, in Routledge International Handbook of Participatory Design. New York: Routledge. doi: 10.4324/9780203108543-11.

Robertson, T. and Wagner, I. (2013b) *'Ethics: engagement, representation and politics-in-action'*, in Routledge International Handbook of Participatory Design. Routledge, pp. 64–85. Available at: https://opus.lib.uts.edu.au/handle/10453/28278 (Accessed: 4 July 2020).

Rode, J. A. and Poole, E. S. (2018) *'Putting the gender back in digital housekeeping'*, in Proceedings of 4th Conference on Gender & IT 2018. Conference on Gender & IT 2018, Heilbronn, Germany. doi: 10.1145/3196839.3196845.

Rohracher, H. (2003) *'The Role of Users in the Social Shaping of Environmental Technologies'*, Innovation: The European Journal of Social Science Research, 16(2), pp. 177–192. doi: 10.1080/13511610304516.

Rubin, J. D., Blackwell, L. and Conley, T. D. (2020) *'Fragile Masculinity: Men, Gender, and Online Harassment'*, in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI '20), pp. 1–14. doi: 10.1145/3313831.3376645.

Ryen, A. (2004) *'Ethical issues'*, Qualitative research practice, pp. 230–247.

Saldana, J. (2015) The Coding Manual for Qualitative Researchers. 1st edn. SAGE.

Sambasivan, N., Weber, J. and Cutrell, E. (2011) *'Designing a phone broadcasting system for urban sex workers in India'*, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 267–276.

Sanders, E. B.-N. and Stappers, P. J. (2008) *'Co-creation and the new landscapes of design'*, Co-design, 4(1), pp. 5–18.

Schnurr, M. P., Mahatmya, D. and Basche III, R. A. (2013) *'The role of dominance, cyber aggression perpetration, and gender on emerging adults' perpetration of intimate partner violence.'*, Psychology of violence, 3(1), p. 70.

Schon, D. A. (1991) The reflective practitioner: How professionals think in action. Ashgate.

Schuler, D. and Namioka, A. (1993) Participatory design: Principles and practices. CRC Press.

Shahani, A. (2014) Smartphones Are Used To Stalk, Control Domestic Abuse Victims, NPR. Available at: https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims (Accessed: 20 March 2018).

Shankar, K. et al. (2012) *'Aging, Privacy, and Home-Based Computing: Developing a Design Framework'*, IEEE Pervasive Computing, 11(4), pp. 46–54. doi: 10.1109/MPRV.2011.19.

Shevat, A. (2017) Designing Bots: Creating Conversational Experiences. 1st Edition. O'Reilly Media, Inc.

Shin, J., Park, Y. and Lee, D. (2018) *'Who will be smart home users? An analysis of adoption and diffusion of smart homes'*, Technological Forecasting and Social Change, 134, pp. 246–253. doi: 10.1016/j.techfore.2018.06.029.

Simonsen, J. and Robertson, T. (2012) Routledge international handbook of participatory design. Routledge. Available at: https://books.google.co.uk/books?hl=en&lr=&id=l29JFCmqFikC&oi=fnd&pg=PP2&dq=Routledge+International+Handbook+of+Participatory+Design&ots=Vpgo0rhYNV&sig=q0FMRzhZr8vpOP-Xp0AXPmN5kwU (Accessed: 10 February 2017).

Snook, Chayn, and SafeLives (2017) Tech vs Abuse: Research Findings. Comic Relief. Available at: https://www.techvsabuse.info/research-findings.

Sørensen, K. H. (1994) *'Technology in use: Two essays in the domestication of artefacts'*, STS-arbeidsnotat, 2, p. 94.

Southern, J. et al. (2014) *'Imaginative labour and relationships of care: Co-designing prototypes with vulnerable communities'*, Technological Forecasting and Social Change, 84, pp. 131–142. doi: 10.1016/j.techfore.2013.08.003.

Southworth, C. et al. (2007) *'Intimate Partner Violence, Technology, and Stalking'*, Violence Against Women, 13(8), pp. 842–856. doi: 10.1177/1077801207302045.

Spiel, K. et al. (2020) *'In the details: the micro-ethics of negotiations and in-situ judgements in participatory design with marginalised children'*, CoDesign, 16(1), pp. 45–65.

Spitzberg, B. H. and Hoobler, G. (2002) *'Cyberstalking and the technologies of interpersonal terrorism'*, New Media & Society, 4(1), pp. 71–92. doi: 10.1177/14614440222226271.

Spot (2019) Harassment training, surveys, and anonymous reporting | Spot. Available at: https://talktospot.com/ (Accessed: 28 December 2019).

Ssozi-Mugarura, F., Blake, E. and Rivett, U. (2017) *'Codesigning with communities to support rural water management in Uganda'*, CoDesign, 13(2), pp. 110–126. doi: 10.1080/15710882.2017.1310904.

Statista (2018a) IoT: number of connected devices worldwide 2012-2025, Statista. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Accessed: 21 March 2018).

Statista (2018b) Smart Home - United Kingdom, Statista Market Forecast. Available at: https://www.statista.com/outlook/279/156/smart-home/united-kingdom (Accessed: 14 September 2018).

Steen, M. (2011) *'Upon opening the black box of participatory design and finding it filled with ethics'*, Nordes, (4).

Strengers, Y. (2016) *'Envisioning the smart home: reimagining a smart energy future'*, Digital materialities: Design and anthropology, 61, pp. 61–76.

Strengers, Y. et al. (2019) *'Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters'*, in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI '19), p. 645:1-645:13. doi: 10.1145/3290605.3300875.

Strengers, Y. and Nicholls, L. (2018) *'Aesthetic pleasures and gendered tech-work in the 21st-century smart home'*, Media International Australia, 166(1), pp. 70–80. doi: 10.1177/1329878X17737661.

Suarez-Villa, L. (2012) Technocapitalism: A Critical Perspective on Technological Innovation and Corporatism. Temple University Press.

Sullivan, C. M. et al. (2008) *'Evaluating the Effectiveness of Women's Refuges: A Multi-Country Approach to Model Development'*, International Journal of Comparative and Applied Criminal Justice, 32(2), pp. 291–308. doi: 10.1080/01924036.2008.9678790.

Svalastog, A.-L. and Eriksson, S. (2010) *'You can use my name; you don't have to steal my story — a critique of anonymity in indigenous studies'*, Developing World Bioethics, 10(2), pp. 104–110.

Tabassum, M. et al. (2020) *'Smart Home Beyond the Home: A Case for Community-Based Access Control'*, in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu, HI, USA: Association for Computing Machinery (CHI '20), pp. 1–12.

Taylor, N. et al. (2013) *'Leaving the Wild: Lessons from Community Technology Handovers'*, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI '13), pp. 1549–1558. doi: 10.1145/2470654.2466206.

The National Commission for the Protection of Human Subjects (1979) The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Appendix. Department of Health, Education, and Welfare.

Thompson, S. (1996) Paying respondents and informants, Social Research Update. Available at: http://sru.soc.surrey.ac.uk/SRU14.html (Accessed: 9 February 2020).

Thorpe, A. and Gamman, L. (2011) *'Design with society: why socially responsive design is good enough'*, CoDesign, 7(3–4), pp. 217–230. doi: 10.1080/15710882.2011.630477.

Tokunaga, R. S. and Aune, K. S. (2017) *'Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking'*, Journal of Interpersonal Violence, 32(10), pp. 1451–1475.

Tolmie, P. and Crabtree, A. (2018) *'The Practical Politics of Sharing Personal Data'*, Personal Ubiquitous Comput., 22(2), pp. 293–315. doi: 10.1007/s00779-017-1071-8.

Towers, J. and Walby, S. (2012) Measuring the impact of Cuts in public expenditure on the provision of services to prevent violence against women and girls. Trust for London. Available at: /publications/measuring-impact-cuts-public-expenditure-provision-services-prevent-violence-against-women-and-girls/ (Accessed: 17 January 2018).

Townsend, M. (2020) *'Revealed: surge in domestic violence during Covid-19 crisis'*, The Observer, 12 April. Available at: https://www.theguardian.com/society/2020/apr/12/domestic-violence-surges-seven-hundred-per-cent-uk-coronavirus (Accessed: 4 July 2020).

Tutenel, P., Ramaekers, S. and Heylighen, A. (2019) *'Conversations between procedural and situated ethics: Learning from video research with children in a cancer care ward'*, The Design Journal, 22(sup1), pp. 641–654. doi: 10.1080/14606925.2019.1595444.

Ugalde, A. (1985) *'Ideological dimensions of community participation in Latin American health programs'*, Social Science & Medicine (1982), 21(1), pp. 41–53.

Velia, H. (2018) *'Who controls the controls?'*, Engineering Technology, 13(6), pp. 44–47. doi: 10.1049/et.2018.0603.

Vesnic-Alujevic, L., Breitegger, M. and Pereira, Â. G. (2016) *'What smart grids tell about innovation narratives in the European Union: Hopes, imaginaries and policy'*, Energy Research & Social Science, 12, pp. 16–26. doi: 10.1016/j.erss.2015.11.011.

Vickery, J. R. (2018) *'This Isn't New: Gender, Publics, and the Internet'*, in Mediating Misogyny: Gender, Technology, and Harassment. Palgrave Macmillan, pp. 31–49.

Vines, J. et al. (2012) *'Questionable concepts: critique as resource for designing with eighty somethings'*, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI '12), pp. 1169–1178. doi: 10.1145/2207676.2208567.

Wachter-Boettcher, S. (2017) Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech. W. W. Norton & Company.

Watkins, L. E., Maldonado, R. C. and DiLillo, D. (2018) *'The Cyber Aggression in Relationships Scale: A New Multidimensional Measure of Technology-Based Intimate Partner Aggression'*, Assessment, 25(5), pp. 608–626. doi: 10.1177/1073191116665696.

Webber, J. E. (2017) Anita Sarkeesian: *'It's frustrating to be known as the woman who survived #Gamergate'*, the Guardian. Available at: http://www.theguardian.com/lifeandstyle/2017/oct/16/anita-sarkeesian-its-frustrating-to-be-known-as-the-woman-who-survived-gamergate (Accessed: 9 April 2018).

Weissman, D. M. (2007) *'The Personal Is Political-and Economic: Rethinking Domestic Violence'*, BYU L. Rev., p. 387.

Westlund, A. C. (1999) *'Pre-Modern and Modern Power: Foucault and the Case of Domestic Violence'*, Signs: Journal of Women in Culture and Society, 24(4), pp. 1045–1066. doi: 10.1086/495402.

Whitham, R. et al. (2019) *'Understanding, capturing, and assessing value in collaborative design research'*, CoDesign, 15(1), pp. 1–7. doi: 10.1080/15710882.2018.1563194.

Willig, C. and Rogers, W. S. (2017) The SAGE handbook of qualitative research in psychology. Sage.

Wilsdon, J. et al. (2015) 'The metric tide: Independent review of the role of metrics in research assessment and management'. doi: 10.13140/RG.2.1.4929.1363.

Wilson, C., Hargreaves, T. and Hauxwell-Baldwin, R. (2015) *'Smart Homes and Their Users: A Systematic Analysis and Key Challenges'*, Personal Ubiquitous Comput., 19(2), pp. 463–476. doi: 10.1007/s00779-014-0813-0.

Winschiers-Theophilus, H., Bidwell, N. J. and Blake, E. (2012) *'Altering participation through interactions and reflections in design'*, CoDesign, 8(2–3), pp. 163–182. doi: 10.1080/15710882.2012.672580.

Women's Aid (2015) Making a safety plan, Women's Aid: until women & children are safe. Available at: https://www.womensaid.org.uk/the-survivors-handbook/making-a-safety-plan/ (Accessed: 23 April 2019).

Woodlock, D. (2016) *'The Abuse of Technology in Domestic Violence and Stalking'*, Violence Against Women, 23(5), pp. 584–602. doi: 10.1177/1077801216646277.

World Health Organisation (2017) Violence against women: Intimate partner and sexual violence against women, World Health Organisation. Available at: http://www.who.int/mediacentre/factsheets/fs239/en/ (Accessed: 17 January 2018).

Zheng, S. et al. (2018) *'User Perceptions of Smart Home IoT Privacy'*, Proc. ACM Hum.-Comput. Interact., 2(CSCW), p. 200:1-200:20. doi: 10.1145/3274469.

A

PARTICIPANT INFORMATION SHEETS

INTERVIEWS

Invitation / Information Sheet

ual: central saint martins

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

What is the purpose of the study?

We invite you to take part in a research study that aims to better understand the individual experiences of people who have been in an abusive relationship. We are collecting information on people's experiences of abuse enabled by technology, such as cyber-stalking and -harassment. The information we gather will contribute to a project investigating the use of digital technologies – such as smartphones, sensors, and connected home devices – to improve the services available to victims of domestic abuse. What we find may be used to develop:

- further information and support for people going through domestic abuse;
- training materials for health, social care, and law-enforcement professionals;
- public presentations and awareness raising events;
- research papers.

Why have you been asked to take part?

You have been contacted because we want to interview people who have experienced domestic abuse that had a component of technology-enabled abuse. We will interview a range of people who have had such experiences.

Who is performing the study?

The researcher's name is Roxanne Leitão. She is undertaking her PhD studies at the University of the Arts London. The supervisory team includes Dr. Matt Malpass and Prof. Lorraine Gamman.

What will you be asked to do?

We will ask you to participate in an interview with the researcher. A trained domestic abuse counsellor will be present, should you need any support. If you choose to participate, we will arrange an interview at a safe time that suits you. The interview will be conducted over Skype. The interview will be video recorded, so the researcher can later analyse the recording instead of taking extensive notes during the interview.

How often and for how long?

The interview will be about 1 hour. There will only be one interview. Once the researcher has analysed the interview and summarised the results, these will be sent back to you so you can review them and let her know if anything was misinterpreted.

When can I discuss my participation?

You can contact the researcher if you are interested in finding out more about the study r.leitao@csm.arts.ac.uk. She will be happy to

discuss it with you and provide more information.

After this, if you choose to participate, there will be a briefing session, before the interview itself. You can choose to leave the study at any point and without giving an explanation.

If you have any concerns about this research, please contact UAL Research Ethics: researchethics@arts.ac.uk.

Who will be responsible for the information?

The information will be securely stored and encrypted by the researcher, even after the study is over.

Who will have access to it?

Only the researcher, Roxanne Leitão, and her supervisors (Dr Matt Malpass, Prof Lorraine Gamman, and Dr Peter Hall) will have access to the data.

How will you use what you find out?

The findings will be used in a PhD project called "Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things". They may also be used in academic publications, presentations, and reports.

Will anyone be able to connect me with what is recorded and reported?

The interview recordings will be anonymised. Nobody will be able to link you to the research.

How long is the whole study likely to last?

The whole study is likely to last another 2 years. The interview will last 45 min to an hour.

Can I find out about the results of the study?

The results will be published on a website hosted by University of the Arts London. You will be given the address of the website directly after the interview.

What if I do not wish to take part or change my mind during the study?

Participating in this study is entirely voluntary. If you wish to participate you can get in touch with Domestic Shelters or email r.leitao@csm.arts.ac.uk. You can withdraw participation at any time, without giving reason. If you do decide to attend the interview, you can choose not to answer the questions, or even end the interview without giving reason if anything is making you uncomfortable.

What support will be in place for me?

Given the nature of this study, it is highly unlikely that you will suffer harm by taking part. However, we have arranged for an experienced domestic abuse counsellor to be present in the interview, just in case you feel that you need support.

If you have any questions, please contact:

Roxanne Leitão

University of the Arts London

r.leitao@csm.arts.ac.uk

If you have any concerns, please contact:

Research Ethics

University of the Arts London

researchethics@arts.ac.uk

Invitation / Information Sheet

ual: central saint martins

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

What is the purpose of the study?

We invite you to take part in a research project that aims to understand the threats that novel technologies may pose to victims of domestic abuse. We are focussing on technology-enabled forms of staking and abuse, as well as what can be done to provide better support to victims going through this.

Why have you been asked to take part?

You have been asked to take part in this study because you are a professional with experience in dealing with cases of domestic abuse.

Who is performing the study?

The researcher's name is Roxanne Leitão. She is undertaking her PhD studies at the University of the Arts London. The supervisory team includes Dr. Matt Malpass and Prof. Lorraine Gamman.

What will you be asked to do?

We will ask you to participate in a one-to-one interview with the researcher. The interview will be video recorded, so the researcher can later analyse the recording, instead of taking extensive notes during the interview.

All the information will be anonymised so that you cannot be linked back to it.

Where and when will this take place?

The interview will either take place at Central Saint Martins in King's Cross (London) or at the headquarters of the charity that has contacted you, before the end of 2017. If you choose to participate, we will organise a time and date that is most convenient for you.

How often and for how long?

The interview will last about 1 hour. There will only be one interview. Once the researcher has analysed the interview and summarised the results, these will be sent back to you so you can review them and let her know if anything was misinterpreted.

What kind of questions will we ask?

We will ask questions about your professional experience in supporting victims of domestic abuse.

When can I discuss my participation?

You can contact the researcher if you are interested in finding out more about the study r.leitao@csm.arts.ac.uk. She will be happy to discuss it with you and provide more information.

After this, if you choose to participate, there will be a briefing session, before the interview

itself. You can choose to leave the study at any point and without giving explanation.

If you have any concerns about this research, please contact UAL Research Ethics: researchethics@arts.ac.uk.

Who will be responsible for the information?

The information will be securely stored and encrypted by the researcher, even after the study is over.

Who will have access to it?

Only the researcher, Roxanne Leitão, and her supervisors (Dr Matt Malpass, Prof Lorraine Gamman, and Dr Peter Hall) will have access to the data.

How will you use what you find out?

The findings will be used in a PhD project called "Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things". They may also be used in academic publications, presentations and reports.

Will anyone be able to connect me with what is recorded and reported?

The interview recordings will be anonymised. Nobody will be able to link you to the research.

How long is the whole study likely to last?

The interview will last an hour. It is part of a larger study that is likely to last a further 2 years.

Can I find out about the results of the study?

The results will be published on a website hosted by University of the Arts London. You will be given the address of the website after the interview.

What if I do not wish to take part or change my mind during the study?

Participating in this study in entirely voluntary. If you wish to participate you can get in touch with the person who sent you this email, or email r.leitao@csm.arts.ac.uk. You can withdraw participation at any time, without giving reason. If you do decide to attend the interview, you can choose not to answer the questions, or even to end the interview without giving reason.

If you have any questions, please contact:

Roxanne Leitão

University of the Arts London

r.leitao@csm.arts.ac.uk

If you have any concerns, please contact:

Research Ethics

University of the Arts London

researchethics@arts.ac.uk

B

CONSENT FORM

INTERVIEWS

ual: central saint martins

Consent Form

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

Please answer the following questions by ticking the response that applies.

1. I have read the Information Sheet and the study has been explained to me. ◯

2. My questions about the research have been answered to my satisfaction and I understand that I may ask further questions at any point. ◯

3. I understand that I am free to withdraw from the interview, without giving a reason for my withdrawal or to decline to answer any particular questions without any consequences to my future treatment by the researcher. ◯

4. I agree to provide information under the conditions of confidentiality set out in the Information Sheet. ◯

5. I wish to participate under the conditions set out in the Information Sheet. ◯

6. I consent to the information collected during this study, once anonymised (so that I cannot be identified), being used for other research purposes. ◯

7. I consent to the information collected during this study, once anonymised (so that I cannot be identified), being used to raise awareness of domestic abuse and to train professionals. ◯

8. I consent to the researcher owning the data gathered in this interview. ◯

9. I consent to being contacted about future research related to this project. ◯

Your name	Your signature	Date

Researcher's name	Researcher's signature	Date

If you have any questions, please contact:

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

If you have any concerns, please contact:

Research Ethics
University of the Arts London
researchethics@arts.ac.uk

C

PARTICIPANT INFORMATION SHEETS

CODESIGN WORKSHOPS

Invitation/ Information Sheet

Arts & Humanities Research Council

ual: central saint martins

DESIGN AGAINST CRIME Research Centre

London Doctoral Design Centre

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

What is the purpose of the study?

We invite you to take part in a research workshop to brainstorm and prototype ways for victims of domestic abuse and stalking to stay safe online. In order to do so, you will be asked to engage in discussion with other survivors and support workers during the workshop. The results of the workshop will be useful in several ways:

- To develop further information and support for people going through intimate surveillance;
- To support improvement in the services offered to victims;
- To develop training materials for health, social care, and law-enforcement professionals;
- To be used in public presentations and awareness raising events;
- To write research papers.

Why have you been asked to take part?

You have been contacted because of your participation in a domestic abuse support group.

What will you be asked to do?

You will be asked to participate in a workshop, in groups of 4-6 people. Collaboratively, you will be discussing challenges facing victims and survivors with regards to technology and stalking.

Where and when will this take place?

The workshop will take place at the West Norfolk Deaf Association, Railway Rd, King's Lynn PE30 1N on Monday 11th March.

When can I discuss my participation?

If you would like to discuss your partic-ipation you can contact the researcher, Roxanne, at r.leitao@csm.arts.ac.uk. She will be happy to discuss it with you and provide more information. If you have any concerns about the study, you can contact Research Management at the Univer-sity of the Arts London – researchethics@arts. ac.uk.

Who will be responsible for the information?

The information will be securely stored and encrypted by the researcher, even after the study is over.

Who will have access to it?

Only the researcher, Roxanne Leitão, and her supervisors (Dr. Matt Malpass, Prof. Lorraine Gamman, and Dr. Peter Hall) will have access to the data.

How will you use what you find out?

The findings will be used in a PhD project called “Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things”. They may also be used in articles, academic publications, presentations, dissemination materials, and reports.

How long is the whole study likely to last?

This is part of a larger study that is likely to last another 1 year.

Can I find out about the results of the study?

The results will be published on a website hosted by the University of the Arts London.

What if I do not wish to take part or change my mind during the study?

Participating in this study is entirely voluntary. If you wish to participate you can get in touch with the person who sent you this email, or email r.leitao@csm.arts.ac.uk. You can withdraw participation at any time, without giving a reason. If you do decide to attend, you can choose not to cease participation without giving a reason.

If you have any questions, please contact:

Roxanne Leitão

University of the Arts London

r.leitao@csm.arts.ac.uk

If you have any concerns, please contact:

Research Ethics

University of the Arts London

researchethics@arts.ac.uk

D

CONSENT FORM

CODESIGN WORKSHOPS

ual: central saint martins

Consent Form

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

Please answer the following questions by ticking the response that applies.

1. I have read the Information Sheet and the study has been explained to me. ◯

2. My questions about the research have been answered to my satisfaction and I understand that I may ask further questions at any point. ◯

3. I understand that I am free to withdraw from the study, without giving a reason for my withdrawal or to decline to answer any particular questions without any consequences to my future treatment by the researcher. ◯

4. I agree to provide information under the conditions of confidentiality set out in the Information Sheet. ◯

5. I wish to participate under the conditions set out in the Information Sheet. ◯

6. I consent to the information collected during this study, once anonymised (so that I cannot be identified), being used for other research purposes. ◯

7. I consent to my picture being taken, in group settings, during the course of the workshop, with the understanding that it will not be publicly distributed, unless adequately anonymised. ◯

8. I consent to the data, gathered in this workshop, being owned by the researcher. ◯

9. I agree to behave in a manner that is respectful of the participants involved in this workshop, and to be mindful of the effects that my words and actions may have on others. ◯

Your name	Your signature	Date
_____	_____	_____
Researcher's name	Researcher's signature	Date
_____	_____	_____

If you have any questions, please contact:

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

If you have any concerns, please contact:

Research Ethics
University of the Arts London
researchethics@arts.ac.uk

E

REFUGE REPORT

INTERVIEWS & FOCUS GROUPS WITH SURVIVORS

27th February 2019

Survivors' Experiences of Tech Abuse Consultations
Feedback on chatbots

Introduction

Refuge recently carried out consultations on the use of technology to abuse, entitled Survivors' Experiences of Tech Abuse. Over a series of one-to-one interviews and focus groups, survivors in Refuge's services were asked what technology they used, whether technology had been used to abuse them, what impact the abuse had on them, and what they would recommend Refuge, the government, and tech companies do to better support survivors.

During the consultations, survivors were specifically asked whether they thought it would be helpful for Refuge to have a chatbot on their website. They were also asked additional questions which might be used to gain information on what survivors would like to see on a chatbot. The purpose of this was for Refuge to gain information on whether survivors liked the idea of the organisation installing a chatbot on their website, whether it is something they think they would use, and what they might want to use it for. Refuge will use this information to decide whether to install a chatbot and, if so, what content users want from it.

Structure

The Survivor Engagement Coordinator consulted a total of 12 survivors in one-to-one semi-structured interviews. These were conducted face-to-face, with one being conducted over the phone. They lasted, on average, one hour. A total of 36 survivors were consulted over 5 focus groups which lasted, on average, one and a half hours.

One-to-one interviews were conducted first and participants were asked the following questions which may be relevant to gaining information on chatbots:

1. Is there a way that we can make information more easily available? Or make help easier to access? (Either by using technology or not?)
2. Refuge is thinking of having a chatbot on their website. This would appear as a box in the corner of the webpage where you could type a question. A computer-generated response would then provide guidance or 'how-to' notes on how to stay safe or get help. Do you think this is something that would be helpful? Is it something you think you might use?
3. Is there anything you think Refuge could do better to help women experiencing tech abuse?

After these interviews, Jane Keeper, Director of Operations, Roxanne Leitao, PhD Researcher at the University of the Arts London, and Carole Baillie, Survivor Engagement Coordinator, developed a

question which aimed to gather information that would be useful when developing a chatbot. The following question was decided upon:

> "If you were looking online for support because someone is using you or your children's phone, online accounts or any other technology to abuse, stalk or harass you, what support or information would you need most?"

This question was added to the IMPACT casework management system and should appear on all open cases, prompting Refuge staff to ask all service users. The purpose of this was also explained to Service Managers so that they could discuss with staff and encourage responses. The Survivor Engagement Coordinator conducted 5 focus groups and asked this question, or a version of this question, at 4 of the focus groups.

We focused on the experiences of survivors who fit into the following three categories, as they may be considered particularly vulnerable and may have their experiences overlooked:

- young survivors aged 25 and below
- survivors with disabilities and illnesses that impact their ability to complete day-to-day tasks (both mental and physical disabilities and illnesses)
- Survivors of Black, Asian, minority ethnic and refugee (BAMER) backgrounds

Results from consultations

Number of women asked in one-to-one interviews: 8

- Number that believe it would be helpful: 3
- Number that believe it might be helpful/somewhat helpful: 4
- Number that do not think it would be helpful: 1 (because she preferred live chat)

Number of women asked in focus groups: 30

- All of the groups generally said yes they think it would be helpful, no one spoke out to say they did not think it would be helpful
- In one group there was a discussion about how this should not replace the advice that refuge workers give a woman over the phone before coming to refuge. As people are in a panic when fleeing, they are unable to think clearly to go onto a chatbot. Participants felt it was important to walk women through it step by step over the phone (for example how to turn off your location settings, what documents to bring, etc.).

'Do you think a chatbot would is something that would be helpful?'

- Thinks it might be helpful - it would be a silent way to seek help
- "Would be somewhat helpful for short-term questions" – for quick information, but not for long-term, complex support.
- If it could happen in an app that would be great, but if not she still thinks it would be useful. She suggests Refuge posts on their social media accounts that they have a chatbot and provide links to the webpage. The chatbot should be mobile friendly as young people tend to use their phones (this survivor was under-18).

- It would be especially helpful if it answered with simple diagrams. The tech abuse team gave her many documents on how to secure her devices, but some quick diagrams on the chatbot would be more straightforward for people quickly looking for help.
- She said she finds live chat helpful. Sometimes you feel anxious speaking to a person on the phone so typing is better (she suffers from an anxiety disorder). If you're really upset you don't want to be crying over the phone. She also believes live chat could be helpful for women living in refuges. For ex. you might not want to speak to the staff there that you see every day about something embarrassing. Perhaps you don't have enough money for food and don't want to ask them for a food voucher, maybe you could use the live chat even within Refuge so it's anonymous and they can make a referral for you. She would use live chat.
- She thinks it could be helpful. However, someone is unlikely to type in 'how do I turn off my location settings on my phone' because they are unlikely to know that they *need* to do that. Perhaps the chatbot could give people more general advice on 'steps on how to get safe' then within that it could give advice on location settings.
- It would be good if there was some way it could tell that someone was in crisis and needed to speak to a human, then a human could type to them or call them.
- Refuge needs to be careful that the information it is providing on the chatbot cannot be used by a perpetrator to learn new ways to abuse.
- It should include really simple steps and diagrams. Make it easy.
- This could be useful for women once they have moved out of refuge too as they will not have the support worker there to tell them how to secure devices.

What information or help do you think the chatbot should provide?

- Answer questions such as: 'What refuge has space in London?' and 'What time is best to call the NDVH?' This woman spent a lot of time trying to call the helpline and find a refuge space and believes that if a person could look online to find this out it would be much better.
- Signposting to other organisations where appropriate, for ex. to Samaritans.
- 'Find my iPhone' – does it work when phone is turned off? When can someone track you with your phone?
- Spyware – what is it? How does it work? How can you tell that it is on your device? What to do if you think it is on your device
- Latest issues to be aware of
- Before you know you are in an abusive relationship, signs that you might be and details on different types of abuse
- Tips for people who have family members who are experiencing abuse. This woman's mother searched online and could not find any advice. The woman said that the way her mum acted actually made the abuse worse. We discussed how there is similar information online for family of people with drug addictions.
- What is legal/illegal around tech abuse but also DV (especially for people who have come from another country). This should include what is legal/illegal around children, for example can my abusive ex-partner post photos of our child on social media?
- Information on how to secure your children's devices.
- General information on how to secure devices, especially because kids could play with your phone and change the settings and you need to figure out how to change them back.
- How to clear browsing history.
- How to secure the router.
- Suggestions on safer alternative apps to use

- List of the ‘scary’ apps, what they can/can't do
- Make people more aware of Amazon Echo. It knows your location because it needs to tell you the weather. You can also drop in on another room, like a baby monitor, to hear and see (if you have one on a screen) what's going on in the other room. This woman does not know how to make it secure so she's decided not to plug it in.
- Tell people that they can set up their email so that they can login with their phone.
- Google maps - once you invite someone they can check your whole location history. Make sure and turn off.
- Tell people they have to delete friends of friends on Facebook too.
- People should know that they can change their number even if they're in the middle of a phone contract. This is not common knowledge.
- There's software called Jailbreak and it can break into anything except Apple products, one woman claims.
- One woman said that her phone is somehow linked to a TV in another room. She watched tv on her phone at 6am and it turned on the TV in someone else's room and started playing the show. She does not know how this technology works and think this could be explained.
- You can call up any internet provider and tell them you do not want any content 18+ to be allowed, so that kids can't see it.
- There is a call recorder app that records all of the phone calls you have. Can this be admissible evidence in court?

Awareness-raising

When asked what Refuge could do to provide better support to women suffering abuse/tech abuse, they commonly said that awareness-raising was important. Although these points have not been directly suggested for the chatbot, perhaps they are relevant.

- Tell people what a refuge is. Many people had never heard of it until they had to move into one.
- It would be good if Refuge could improve the perception of what a refuge is like. Before moving in, this woman had an image of a refuge being cramped with rooms full of bunk beds. She believes it could help people make the choice to move into refuge if they know that they can have their privacy and that it is quite comfortable.
- A few women who spoke limited English said that it was difficult for them to search online. They suggest that Refuge have information in other languages (for example, Urdu, Dari, French). They often do not know what the word would be in English because terms like ‘domestic abuse’ do not exist in their language.

Conclusion

The survivors consulted overwhelmingly felt that it was a good idea for Refuge to add a chatbot to their website. They came up with many recommendations for information that could be included for women seeking advice and information. They also raised a number of issues which will need to be considered when devising a chatbot to ensure that it is widely accessible to the people who need it the most. This feedback should be considered in combination with the feedback recorded on Refuge’s casework management system in order to provide the best version of a chatbot to survivors visiting the site.

F

REFUGE REPORT

CROSS-PLATFORM TESTING

Document	Chatbot Test	Date	2nd October 2019
Version	1.00.00	Completed by	Alan Owen
Distribution	Director of Operations	Usage	Testing
Details	Chatbot testing report – All devices – All options		

Contents

Introduction

This document reports the findings of the testing process on the new Refuge Chatbot. Each option and video has been tested by 2 separate people across 2 days.

The following devices were used for testing the Chatbot:

Device	Operating System
Samsung S9+	Android
Apple iPhone 10	IOS
Samsung Galaxy Tab S4	Android
Apple iPad	IOS
Microsoft Surface Laptop	Windows 10

The chatbot was accessed via the URL: http://roxanneleitao.com/bot.html

The following user interfaces were also analysed:

- Mobile Compatibility
- YouTube integration
- Speed
- Menu structure
- Menu navigation
- Spelling mistakes
- Consistency of wording

iPhone Videos / Section

Device	Section	Sub-section	Findings
iPhone	Location Settings	Find my friends	Asks to open settings, but does not explain settings
		Find my iPhone	Explains the settings icon is the cog. Needs consistency throughout videos. Shows the refuge.org.uk email address and shows password. (I am assuming that the password has since been changed)
		Family Sharing	No Issues
		Facebook	No Issues
		Instagram	No Issues
		Twitter	No Issues
		Google Maps	No Issues
	Social Media - Facebook	Who's logged in	No Issues
		Who sees my posts	No Issues
		Change my password	Shows password. (I am assuming that the password has since been changed)
		Block someone	No Issues
		Disable location	No Issues
	Social Media – Instagram	Who sees my posts	No Issues
		Change my password	Shows password. (I am assuming that the password has since been changed)
		Block someone	No Issues
		Turn off location	No Issues
	Social Media – Twitter	Who sees my posts	No Issues
		Change my password	No Issues
		Block someone	No Issues
		Turn of location	No Issues
	iCloud / Apple ID	Who's got access	No Issues
		Change my password	No Issues
		Family sharing	No Issues

Android Videos / Section

Device	Section	Sub-section	Findings
Android	Location Settings	Facebook	No Issues
		Instagram	No Issues
		Snapchat	No Issues
		Twitter	Video unavailable. Also has link for full screen video?
		Google Maps	No Issues
	Social Media – Facebook	Who's logged in	No Issues
Android	Social Media - Facebook	Who sees my posts	No Issues
		Change my password	No Issues
		Block someone	No Issues
		Disable location	No Issues
	Social Media – Instagram	Who sees my posts	No Issues
		Change my password	No Issues
		Block someone	No Issues
		Disable my location	No Issues
	Social Media – Snapchat	Who sees my posts	No Issues
		Change my password	No Issues
		Block someone	No Issues
		Turn off location	No Issues
	Social Media – Twitter	Who sees my posts	No Issues
		Change my password	No Issues
		Block someone	No Issues
		Turn off location	Has link for full screen video?

Overall findings / recommendations

The following overall findings were recorded during testing:

Finding	Issue	Recommendation
Setting icon on Video	Some videos mention the setting icon / app and show it, others just say click settings.	Give a consistent message and explain how to get to the settings icon.
Fullscreen link	Some videos have a full screen message, others do not.	Give a consistent message for full screen. We found no need to show the full screen message.
Menu navigation	Cannot return to the start, you have to click the three lines at the bottom of the screen and click return to main menu.	Needs a restart button on each option, if you choose the wrong phone at the start, you either have to click the three lines or close and start again.
Menu navigation	When in a particular section, such as Facebook, the navigation take you back to choosing the main topic and then to the section again.	For example, in iPhone, Social Media – Facebook, you have to click the menu 20 times to change each setting. Can the menu be changed so that when you are in a section, you easily click each option, rather than returning to the main menu?
Menu navigation	The main menu asks, "what can I help with" and then the phone type. Once phone type has been chosen, you cannot change it without restarting.	Can we change the menu to ask for phone first and give an option to return to phone type?
Menu navigation	Main menu button does not return to the start	The main menu does not return to main menu, just to a sub menu. Need to redesign the buttons so that sections and start again can be chosen.
YouTube	When a YouTube video has finished, you are presented with adverts for videos which are not relevant.	Consider hosting the videos on the new Helpline web site so that videos do not contain suggestions for other videos at the end.
Videos	The videos do not end with any standard credits.	Should there be a final screen with details of the helpline and how to call it on each video?

Conclusion

The Chatbot performed extremely well on every device that it was tested on, there were no issues with the functionality on any operating system or device.

The videos are now at the correct speed and are very easy to follow, although a final screen with the helpline number / contact details would make the message consistent throughout.

The menu navigation does need to be reworked, when changing every setting for a particular section (Facebook for example) the process to access all of the videos is time consuming and may put off potential users.

A decision needs to be made as to where the videos are stored, due to the advertising of potential videos on YouTube.

Only one video failed to display (Android – Location Settings – Twitter).

Once the menu's have been reworked for easier access and a decision on the video platform, this chatbot will give an invaluable service to anyone looking to protect their security across their mobile devices, across multiple applications.

G

PARTICIPANT INFORMATION SHEETS

CO-EVALUATION

Invitation/ Information Sheet

ual: central saint martins

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

What is the purpose of the study?

We invite you to take part in the evaluation of a chatbot prototype. The chatbot is intended to provide advice, to victims, on how to manage digital privacy and security. What we develop in the workshop will be useful in several ways:

- To improve the chatbot;
- To develop further information and support for people going through domestic abuse;
- To support improvement in the services offered to victims;
- To be used in public presentations and awareness raising events;
- To write research papers.

Why have you been asked to take part?

You have been contacted because of your participation with Refuge.

What will you be asked to do?

We will ask you to participate in a feedback session, which will last 15-20 minutes. You will be using the chatbot and letting us know what you think.

When can I discuss my participation?

If you have any concerns about the study, you can contact Research Management at the University of the Arts London – researchethics@arts.ac.uk. If you would like to discuss your participation you can contact the researcher, Roxanne, at r.leitao@csm.arts.ac.uk. She will be happy to discuss it with you and provide more information.

Who will be responsible for the information?

The information will be securely stored and encrypted by the researcher.

Who will have access to it?

Only the researcher, Roxanne Leitão, will have access to the data.

How will you use what you find out?

The findings will be used by Refuge to inform the development of the chatbot. They will also be used in a PhD project called “Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things”. They may also be used in articles, publications and presentations.

How long is the whole study likely to last?

This is part of a larger study that is likely to last another 6 months.

What if I do not wish to take part or change my mind during the study?

Participating in this study is entirely voluntary. You can withdraw participation at any time, without giving a reason. If you do decide to attend, you can choose not to cease participation without giving a reason.

Can I find out about the results of the study?

The results will be published on a website hosted by University of the Arts London.

If you have any questions, please contact:

Roxanne Leitão

University of the Arts London

r.leitao@csm.arts.ac.uk

If you have any concerns, please contact:

Research Ethics

University of the Arts London

researchethics@arts.ac.uk

CONSENT FORM

CO-EVALUATION

ual: central saint martins

Consent Form

Research Project Title

Codesigning Support Solutions for Victims of Cyberstalking and Abuse: reclaiming privacy and safety on the Internet of Things

Please answer the following questions by ticking the response that applies.

1. I have read the Information Sheet and the study has been explained to me. ◯

2. My questions about the research have been answered to my satisfaction and I understand that I may ask further questions at any point. ◯

3. I understand that I am free to withdraw from the study, without giving a reason for my withdrawal or to decline to answer any particular questions without any consequences to my future treatment by the researcher. ◯

4. I agree to provide information under the conditions of confidentiality set out in the Information Sheet. ◯

5. I wish to participate under the conditions set out in the Information Sheet. ◯

6. I consent to the information collected during this study, once anonymised (so that I cannot be identified), being used for other research purposes. ◯

7. I consent to my picture being taken, with the understanding that it will not be publicly distributed, unless adequately anonymised. ◯

8. I consent to the data, gathered in this workshop, being owned by the researcher. ◯

9. I agree to behave in a manner that is respectful of the participants involved in this workshop, and to be mindful of the effects that my words and actions may have on others. ◯

Your name	Your signature	Date
_____	_____	_____
Researcher's name	Researcher's signature	Date
_____	_____	_____

If you have any questions, please contact:

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

If you have any concerns, please contact:

Research Ethics
University of the Arts London
researchethics@arts.ac.uk